Steve D. Larson, OSB No. 863540
Email: slarson@stollberne.com
Jennifer S. Wagner, OSB No. 024470
Email: jwagner@stollberne.com
STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 SW Oak Street, Suite 500
Portland, Oregon 97204
Telephone: (503) 227-1600

Attorneys for Plaintiffs

[Additional Counsel Listed on Signature Page.]

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

BLUE PEAK HOSTING, LLC, PAMELA GREEN, TITI RICAFORT, MARGARITE SIMPSON, and MICHAEL NELSON, on behalf of themselves and all others similarly situated, Plaintiffs, v. INTEL CORPORATION, a Delaware corporation, Defendant.	Case No. **CLASS ACTION ALLEGATION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Blue Peak Hosting, LLC, Pamela Green, Titi Ricafort, Margarite Sampson, and Michael Nelson, individually and on behalf of the members of the Class defined below, allege the following against Defendant Intel Corporation ("Intel" or "the Company"), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, the investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. Despite Intel's intentional concealment of specific design choices that it long knew rendered its central processing units ("CPUs" or "processors") unsecure, it was only in January 2018 that it was first revealed to the public that Intel's CPUs have significant security vulnerabilities that gave unauthorized program instructions access to protected data.

2. A CPU is the "brain" in every computer and mobile device and processes all of the essential applications, including the handling of confidential information such as passwords and encryption keys. Maintaining the security of confidential information is a fundamental function of all CPUs that Plaintiffs and members of the Class relied upon Intel to provide. "Processor-level security is foundational and can prevent the exploitation that software-based products can be prone to."[1] Indeed, the CPU "plays a fundamental role in security because of performance, hardware-rooted trust, and the ability to provide security functionality, such as encryption, while exposing minimal attack surface area."[2]

3. Although Plaintiffs and members of the Class relied upon Intel to design its CPUs to ensure that private data remains secure from access by unauthorized parties, increased sales, and

[1] See John Abbott, *Trusting in the CPU: Getting to the Roots of Security*, June 2017 at p. 4.

[2] *Id*. at p. 9

thus increased profits, drove Intel to implement certain techniques, such as speculative execution and out-of-order execution, in a manner that left users' confidential information exposed and vulnerable to unauthorized access.

4. In a nutshell, speculative execution allows a CPU to run instructions from software programs or applications before knowing whether an instruction is required or whether access to information is authorized. Intel's defective implementation of "speculative execution" maintains accessed user information, including confidential information, within the CPU (a fast memory known as Cache, and several internal buffers including the Line Fill Buffers, Store Buffers, and Writeback buffers associated with the Cache) in a vulnerable manner, and thus exposes user data to a substantial security risk of exposure and theft by unauthorized third parties.

5. The exploits identified in 2018, generally dubbed "Meltdown," "Spectre," and "Foreshadow" (and related variants), are part of a class of exploits that allow unauthorized third parties to exploit Intel's processor vulnerabilities to gain access to confidential information. The exploits take advantage of design defects in Intel's CPUs related to memory access protection and speculative execution of computer program instructions, which made information that should otherwise remain secure accessible to unauthorized use. Unbeknown to Plaintiffs and members of the Class, when Intel's processors engage in speculative execution, the processors make information, which should remain secure and inaccessible to unauthorized use, accessible in the processors' unsecured subsystems. These undisclosed design defects, which Plaintiffs define herein as "Unauthorized Access" and "Incomplete Undo" (the "Defects"), are exploited by an ever-increasing number of exploits as hackers gain additional insight into the Defects.

6. As designed, Intel CPUs suffer from Unauthorized Access which allows program instructions unauthorized access to protected data (e.g., secrets). When Intel processors

speculatively execute instructions, Incomplete Undo allows protected data to remain in Intel's CPU's unsecure subsystems (e.g., those instructions are not completely undone) when speculation is wrong. Intel was aware that its processor design, which allowed secrets to be placed into the CPU's unsecure subsystems by unauthorized users, presented a substantial security risk to consumers and could be exploited.

7. More troubling, Intel's flawed processor design affects almost every x86-64 Core processor CPU that Intel designed, manufactured, marketed, sold, and distributed in the last 20 years ("Intel's CPU(s)").

8. Because Intel has failed and refused to address the underlying Defects in Intel's CPUs, additional exploits, dubbed "Fallout," "RIDL," and "ZombieLoad" (and related variants) by the researchers (and referred to collectively by Intel as Microarchitectural Data Sampling ("MDS")) as well as SwapGS and LazyFP were disclosed in 2019. Even more exploits, dubbed "Vector Register Sampling," "CacheOut," and "Snoop-assisted L1 Data Sampling" were disclosed in 2020. All of these exploits exploit the same undisclosed Defects in Intel's CPU design and have been discovered on an ongoing basis for over two years, with the most recent one reported in March 2020. Undoubtedly, more exploits exploiting the Defects are expected and will continue to be disclosed. Fallout, RIDL, ZombieLoad, SwapGS, LazyFP, Vector Register Sampling, CacheOut, Snoop-assisted L1 Data Sampling, and the yet-to-be-disclosed exploits are referred to collectively with Meltdown, Spectre, and Foreshadow as the "Intel CPU Exploits."

9. The Defects that allow the Intel CPU Exploits are the direct result of Intel's knowing decision to sacrifice security in favor of speed to gain an edge in its ongoing competition with rivals such as Advanced Micro Devices, Inc. ("AMD"). As with the Meltdown and Foreshadow exploits, Fallout, RIDL, ZombieLoad, SwapGS, LazyFP, Vector Register Sampling, and CacheOut exploit

Intel-processor Defects. AMD has reported that its processors are not subject to Meltdown, Foreshadow, Fallout, RIDL, ZombieLoad, SwapGS, LazyFP, Vector Register Sampling, and CacheOut. Despite Intel's efforts to mischaracterize the Defects and the Intel CPU Exploits as industry-wide risks of chip manufacturers, the truth is that only Intel designed its CPUs in this flawed manner and, because of its design choices, the Intel CPU Exploits are largely an Intel-only problem.

10. Moreover, Intel's decision to forego security for the sake of speed was contrary to the public statements it made about the security of its processors. Although Intel publicly touted its processors' security, Intel kept its hardware design strictly confidential, within its exclusive knowledge, and actively protected as a trade secret. Plaintiffs and members of the Class had no way of knowing before their purchases that Intel disregarded a fundamental CPU function—data security—and knowingly designed its CPUs to permit unprotected memory access during speculative execution.

11. Executing the Intel CPU Exploits leaves no fingerprints or forensic trace and are thus exceptionally hard to detect. "But [it is] suspect[ed] that for intelligence agencies and commercial hacking groups, Meltdown and Spectre [as well as the other Intel CPU Exploits] are already parts of their toolkits; they're probably paired with fileless malware as an entry point. With fileless malware, nothing is written to disk, and with Meltdown [and the other Intel CPU Exploits], there's reportedly no need for privilege escalation. The result is a super-stealthy exploit that is less likely

to trigger any alarms."[3] Even Intel acknowledged that the Intel CPU Exploits could "be maliciously exploited in the wild by highly sophisticated cyber-criminals."[4]

12. While programs without the requisite permission should not be allowed to read data associated with other programs, unauthorized users can exploit the Defects to get hold of secrets stored in the memory of other running programs. This might include confidential or personal information such as passwords stored in a password manager or web browser, personal photos, emails, instant messages and even business-critical documents. For example, by exploiting the Defects, a web page in one browser tab could read a user's online banking password from another browser tab. Or, on cloud servers, one virtual machine could snoop on the data in other virtual machines on the same system. This is not supposed to be possible.

13. Although it has yet to come forth with a full and candid description of all facts known only to it concerning the unprecedented security Defects, what Intel has already admitted is damning. According to Intel, "[t]hese side-channel leaks are particularly dangerous in environments running large numbers of virtualized servers on shared host servers in the cloud. It is problematic because it is possible for an unauthorized virtual machine to eavesdrop on a victim's VM."[5] Acknowledging that its customers are "security conscious," Intel has advised its customers to

---

[3] Mike Fong, *Five Mobile Security Predictions For 2020*, Forbes (Jan. 16, 2020), https://www.forbes.com/sites/forbestechcouncil/2020/01/16/five-mobile-security-predictions-for-2020/#56a5fb822cb6

[4] Maxwell Cooter, *We've secured our CPU silicon, and ready to secure your business, says post-Meltdown Intel*, The Register (Sept. 12, 2019), https://www.theregister.co.uk/2019/09/12/securing_the_silicon/

[5] Maxwell Cooter, *We've secured our CPU silicon, and ready to secure your business, says post-Meltdown Intel*, The Register (Sept. 12, 2019), https://www.theregister.co.uk/2019/09/12/securing_the_silicon/

"deploy only machines with the latest generations of processors inside"—which Intel claims include the necessary security defenses "built in."[6]

14. Unbeknownst to Plaintiffs and members of the Class, Intel has known for years that its proprietary CPU design (which permitted unauthorized memory access during speculative execution) could be exploited by side-channel exploits. Furthermore, Intel has been aware of various methods that would secure its CPUs, yet has failed to implement them. Indeed, research shows that Intel purposefully implemented the Defects (and concealed them), which undermined the security of Intel CPUs simply to achieve a performance advantage over AMD and other competitors.

15. As the leader in the global CPU industry, Intel knows the critical importance of both performance and protecting consumers' sensitive data from unauthorized access. Intel also knows the multitude of harms that foreseeably flow to individual consumers when sensitive data is stolen by criminals, including, among other things, identify theft, fraud, credit and reputational harm, erroneous tax claims, and extortion. Indeed, Intel's success is largely based on the advertised speed and security of its CPUs.

16. While some mitigations with microcode updates, operating system-level fixes, and patches to applications like web browsers have become available to ostensibly eliminate the threat of the publicly disclosed Intel CPU Exploits, the mitigations materially affect the performance of Intel's CPUs for all users and also have been shown to be inadequate in curing the Defects. Each new exploit and each associated mitigation creates an additional layer of performance impact.

---

[6] Maxwell Cooter, *We've secured our CPU silicon, and ready to secure your business, says post-Meltdown Intel*, The Register (Sept. 12, 2019), https://www.theregister.co.uk/2019/09/12/securing_the_silicon/

17. Even worse, to minimize the risk of exploit, it is recommended that users disable key Intel CPU performance functionality altogether, such as Hyper-Threading (which allows a single physical CPU to appear as two logical CPUs to an operating system with the ability to share physical execution resources).[7] That is why Google disabled hyperthreading on its Intel-based Chromebooks.

18. In other words, every Plaintiff's CPU now suffers reduced functionality and performance as a direct result of downloading Intel's mitigations for the Intel CPU Exploits. As a consequence of the material post-mitigation performance and functionality degradation, Plaintiffs' processors' performance is essentially downgraded into the performance of slower lower cost processors.

19. The only true fix is to exchange each defective CPU for a device containing a processor not subject to the security and performance Defects. The fact that Intel has left variants of MDS unpatched for more than 18 months is a byproduct of Intel's piecemeal and incomplete response to the Intel CPU Exploits. Rather than prevent further exploits by correcting the root cause of the exploits (i.e., the Defects), Intel merely provides a superficial patch for the specific exploit as researchers demonstrate yet another variant of the Intel CPU Exploits. As long as Intel continues to only respond with symptomatic fixes, additional exploits like the Intel CPU Exploits will keep happening. As industry experts stress, "[r]esearchers find these things without even trying very hard. And it probably means that other adversaries will find them, too."[8]

---

[7] Stephen Röttger, *Escaping the Chrome Sandbox with RIDL*, Google Project Zero (Feb. 15, 2020), https://googleprojectzero.blogspot.com/2020/02/escaping-chrome-sandbox-with-ridl.html.

[8] A. Greenberg, *Intel is Patching the Patch for the Patch for Its 'Zombieload' Flaw*, Wired (Jan. 27, 2020), https://www.wired.com/story/intel-zombieload-third-patch-speculative-execution/.

20. To be sure, given that Intel has dozens of CVEs[9] reflecting the status "RESERVED," it appears that numerous yet-to-be-disclosed Intel CPU Exploits are known to Intel and have been embargoed for 6 months or more (characteristic of Intel's practice of significantly delayed disclosure of Intel CPU Exploits).

21. Intel's mitigations are mere band-aids. The security Defects need to be fixed at the CPU *hardware* level. As even Intel has acknowledged, "industry experts have long realised that software only solutions simply will not cut the mustard, since they can ultimately be compromised or bypassed in some way. Instead, security needs to be rooted in hardware capabilities that cannot be altered or disabled by malicious code."[10]

22. Incredibly, even after Intel learned that the Intel CPU Exploits were taking advantage of its design Defects, Intel unreasonably delayed disclosing the side-channel exploits for months, thereby increasing exposure, risk, and injury to Plaintiffs and the other Class members. During this delay and before any of the Intel CPU Exploits were made public (and patches made available), and while Intel continued to advertise, market, and sell its known defective CPUs, former Intel CEO Brian Krzanich exercised and sold off nearly 900,000 company shares and stock options—raking in about $24 million—months after being informed of the significant security vulnerability in its flagship CPUs but before Intel publicly disclosed the problem. The stock sale left Krzanich with just 250,000 shares of Intel stock—the minimum that he is required to own under his Intel employment agreement. By withholding the facts concerning the defective CPUs, Intel put its own

[9] "CVE" refers to Common Vulnerabilities and Exposures, a standardized, industry-endorsed list of security vulnerabilities.

[10] Dan Robinson, *Hardware-drive security in the hybrid cloud*, The Register (Nov. 16, 2017), https://www.theregister.co.uk/2017/11/16/hardwaredriven_security_in_the_hybrid_cloud/

interests ahead of the very consumers who placed their trust and confidence in Intel and benefitted itself to the detriment of Plaintiffs and Class members.

23. Since the 1990's, every computer or device sold with an Intel chip has displayed a sticker with the slogan "Intel Inside," to make consumers believe that they were buying a product with the best, fastest and most powerful processor. And with its marketing and advertising, Intel led consumers to believe that each new generation of processors it introduced was faster and higher performing that the previous one. In fact, at the point of sale, whether online or in a brick-and-mortar store, consumers are presented with the specific processer speed for the Intel CPU that is inside. Plaintiffs and Class members had no reason to suspect and could not have reasonably discovered that Intel had sacrificed security for speed, that the CPUs suffered from the Defects or that their computers and devices would suffer significant performance degradation as a result of implementing mitigations necessary to address the Defects.

24. Had Plaintiffs known about the Defects in Intel's CPUs or that Intel's mitigations needed to address the Intel CPU Exploits would materially impact the CPUs' functionality and performance, they would have paid less for them based only on the CPUs' post-mitigation performance (not the promised pre-mitigation performance). Alternatively, because of the influx of new disclosures and uncertainty surrounding future mitigations and burdens of additional performance regressions, Plaintiffs would not have purchased the devices with Intel processors altogether and instead would have purchased a device with AMD's or other competitor's processors (which are reportedly largely immune from the Intel CPU Exploits).

JURISDICTION AND VENUE

25. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy

exceeds the sum of $5,000,000, exclusive of interest and costs, and Intel is a citizen of a State different from that of at least one Class member.

26. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Intel transacts business and may be found in this District.

PARTIES

27. Each and every Plaintiff and each Class member has suffered a concrete and particularized injury, including, but not limited to, loss of the benefit of the bargain and diminished value of their processors, as a result of Intel's concealment of known Defects in its processors and the material performance regression associated with downloading mitigations in order to ameliorate – but not cure – Intel's deficient security and protect their sensitive information. The deterioration in performance suggests an average reduction in value of 15-20% or more.

28. **Plaintiff Blue Peak Hosting, LLC** ("Blue Peak") is organized under the laws of the state of Utah and primarily does business there. Blue Peak provides website hosting and virtual private server hosting to its clients.

29. Blue Peak maintains private, sensitive, and confidential information.

30. In making purchases and deciding to deploy devices containing Intel CPUs, Blue Peak relied on Intel's representations (both direct and indirect) that its CPUs would provide superior performance, speed, and security and were fit for use in its servers, PCs, and other devices that store, process or access sensitive, confidential, and personal information and data. Blue Peak paid for processor performance it did not receive.

31. Blue Peak expected the processors to function as Intel advertised and represented. Implicit in Intel's representations was that its processor would deliver such performance securely,

so that that data would not potentially be exposed to compromise. Any reasonable purchaser would expect that the computing device being purchased would be secure and free from potential exploits.

32. Unknown to Blue Peak, at the time that it purchased the Affected Devices, those Devices were equipped with Intel processors that contained undisclosed Defects that made information, which should have remained secure and inaccessible to unauthorized parties.

33. Blue Peak purchased the Affected Devices on the reasonable, but mistaken, belief that the processor would provide the performance promised, would do so securely, and would retain all of its operating characteristics throughout its useful life. Had disclosures of the Defects in the Intel CPUs, or that mitigations needed to address the Intel CPU Exploits would materially impact the CPU's functionality and performance, been displayed in Intel's advertisements, brochures, bulletins, and on its webpage, Blue Peak would have seen them and no doubt have taken them into account in making its purchasing decisions. In particular, had Blue Peak known about the Defects in Intel's CPUs or that mitigations needed to address the Intel CPU Exploits would materially impact the CPUs' functionality, security, and performance, it would not have bought the Affected Devices containing Intel processors or it would have paid less for them.

34. As a result of the Defects in Intel's CPUs and the mitigations needed to address the Intel CPU Exploits and in order to comply with its duty to protect confidential information and documents, Blue Peak spent significant time and effort researching the Intel CPU Exploits and implementing available mitigations. Additionally, Blue Peak has been injured because it incurred and will continue to incur time and costs because it has been and will continue to be required to, among other things: purchase on an accelerated schedule compared to normal business practices more powerful processors to compensate for decreased performance resulting from disabling hyperthreading; reconfigure its networks to provide increased security from internet accessibility

for those systems containing the most sensitive data; increase monitoring of the Affected Devices, servers, and firewalls for security threats, attacks and breaches; and supplement its network and computing security program(s) with additional security monitoring.

35. As a result of its research regarding the Intel CPU Exploits, Blue Peak understood that to address the security vulnerabilities it must either install patches for its computers and servers or disable hyperthreading on its computers and servers. Blue Peak's research revealed that installing patches would result in reduced processing speed. Accordingly, Blue Peak elected to disable hyperthreading on its computers and servers. After disabling hyperthreading on its computers and servers, however, Blue Peak experienced noticeable decreases in processing speed.

36. Blue Peak's employees spent over 50 hours completing the tasks described above.

37. Based on these direct and indirect representations, Blue Peak has purchased and continues to use a large number of products containing defective Intel processors, including servers and desktop computers.

38. Because the Intel CPU Defects can be mitigated, but not completely fixed, on existing hardware, Blue Peak will continue to be injured by incurring these additional monitoring costs as long as the Affected Devices are deployed as part of its IT infrastructure.

39. Intel's unfair, unlawful, and deceptive conduct in designing, manufacturing, marketing, and selling its processors with the undisclosed Defects has diminished the value of Blue Peak's Intel processors, and Blue Peak did not receive the benefit of its bargain. As detailed in this Amended Complaint, Blue Peak's Affected Devices are worth less than what it paid for them. Moreover, the Defects in the CPUs have increased Blue Peak's costs of its IT operations.

40. **Plaintiff Pamela Green** is a resident and citizen of the State of California. On or about February 4, 2015, Plaintiff bought a new Windows laptop which featured an Intel Core i5-

4200U as the computer's CPU. Plaintiff bought the laptop from Fry's Electronics store. Plaintiff reviewed and relied on the information about the laptop and Intel processor that was displayed in store. Plaintiff purchased, and still owns, this device containing an Intel processor. Plaintiff has heard and/or read that Intel processors were the world's fastest. Plaintiff expected the processor to function as Intel advertised and represented. Implicit in Intel's representations was that its processor would deliver such performance securely, so that that data would not potentially be exposed to compromise. Any reasonable consumer would expect that the computing device being purchased would be secure and free from potential exploits.

41. Plaintiff has used (and continues to use) the Intel device for multitasking—with various applications open at the same time—between word processing, email, and general web browser use. Plaintiff's computer receives periodic updates that include the CPU patches released to date.

42. Unknown to Plaintiff, at the time of its purchase, the laptop was equipped with an Intel processor that contained undisclosed design Defects that made information, which should have remained secure and inaccessible, accessible to unauthorized parties. While security patches were implemented to protect against the Intel CPU Exploits, after January 2018 when the patches were downloaded, Plaintiff experienced material performance degradation, including reduced processing speed. Plaintiff has also experienced difficulty in multitasking, with the laptop slowing significantly and taking several minutes to start up. In addition, as a result of the Defects in Intel's CPUs and Intel's mitigations needed to address the Intel CPU Exploits, Plaintiff spent time and effort researching the Intel CPU Exploits and implementing available mitigations on her Intel device.

43. Plaintiff paid for processor performance that she did not receive.

44. Intel's unfair, unlawful, and deceptive conduct in designing, manufacturing, marketing, and selling its processors with the undisclosed Defects has diminished the value of Plaintiff's Intel processor and Plaintiff did not receive the benefit of the bargain. After disclosure of the Intel CPU Exploits, it became well known in the market that processor performance of Intel's CPUs would be negatively impacted—across the board—as a result of the necessary patches to secure data from the Intel CPU Exploits due to the undisclosed Defects in the CPUs. Plaintiff's Intel CPU is worth less than what she paid for it.

45. Plaintiff purchased a device containing the Intel processor on the reasonable, but mistaken, belief that the processor would provide the performance promised, would do so securely, and would retain all of its operating characteristics throughout its useful life. Had disclosures of the Defects in the Intel CPUs, or that mitigations needed to address the Intel CPU Exploits would materially impact the CPU's functionality and performance, been displayed in store, Plaintiff would have seen them, and no doubt have taken them into account in making her purchasing decision. In particular, had Plaintiff known about the Defects in Intel's CPUs or that mitigations needed to address the Intel CPU Exploits would materially impact the CPUs' functionality and performance, she would not have bought the laptop containing the Intel processor or would have paid less for it. Plaintiff would have purchased a laptop containing an AMD or other competing processor (which are reportedly immune from the Intel CPU Exploits) or paid only for a device with a CPU delivering the diminished post-mitigation performance (not the promised pre-mitigation performance).

46. **Plaintiff Titi Ricafort** is a resident and citizen of the State of Hawaii. On or about July 16, 2015, Plaintiff bought a new Windows laptop which featured an Intel Core i3-5010U as the computer's CPU. Plaintiff bought the laptop from Best Buy online. Plaintiff reviewed and relied on the information about the laptop and Intel processor that was displayed online. Plaintiff

purchased, and still owns, this device containing an Intel processor. Plaintiff has heard that Intel processors were industry leaders in both performance and security. Plaintiff expected the processor to function as Intel advertised and represented. Implicit in Intel's representations was that its processor would deliver such performance securely, so that that data would not potentially be exposed to compromise. Any reasonable consumer would expect that the computing device being purchased would be secure and free from potential exploits.

47. Plaintiff has used (and continues to use) the Intel device for multitasking between various personal and business tasks, including web browsing, streaming media, storing photographs, and using a virtual private network application. Plaintiff often will have multiple applications open at the same time. Plaintiff's computer receives periodic updates that include the CPU patches released to date.

48. Unknown to Plaintiff, at the time of its purchase, the laptop was equipped with an Intel processor that contained undisclosed design Defects that made information, which should have remained secure and inaccessible, accessible to unauthorized parties. While security patches were implemented to protect against the Intel CPU Exploits, after January 2018 when the patches were downloaded, Plaintiff experienced material performance degradation, including reduced processing speed. Specifically, Plaintiff has experienced frequent freezing while using programs. In addition, as a result of the Defects in Intel's CPUs and Intel's mitigations needed to address the Intel CPU Exploits, Plaintiff spent time and effort researching the Intel CPU Exploits and implementing available mitigations on her Intel device.

49. Plaintiff paid for processor performance that she did not receive.

50. Intel's unfair, unlawful, and deceptive conduct in designing, manufacturing, marketing, and selling its processors with the undisclosed Defects has diminished the value of

Plaintiff's Intel processor and Plaintiff did not receive the benefit of the bargain. After disclosure of the Intel CPU Exploits, it became well known in the market that processor performance of Intel's CPUs would be negatively impacted—across the board—as a result of the necessary patches to secure data from the Intel CPU Exploits due to the undisclosed Defects in the CPUs. Plaintiff's Intel CPU is worth less than what she paid for it.

51. Plaintiff purchased a device containing the Intel processor on the reasonable, but mistaken, belief that the processor would provide the performance promised, would do so securely, and would retain all of its operating characteristics throughout its useful life. Had disclosures of the Defects in the Intel CPU's, or that mitigations needed to address the Intel CPU Exploits would materially impact the CPU's functionality and performance, been displayed online or in the store, Plaintiff would have seen them and no doubt have taken them into account in making her purchasing decision. In particular, had Plaintiff known about the Defects in Intel's CPUs or that mitigations needed to address the Intel CPU Exploits would materially impact the CPUs' functionality and performance, she would not have bought the laptop containing the Intel processor or would have paid less for it. Plaintiff would have purchased a laptop containing an AMD or other competing processor (which are reportedly immune from the Intel CPU Exploits) or paid only for a device with a CPU delivering the diminished post-mitigation performance (not the promised pre-mitigation performance).

52. **Plaintiff Margarite Sampson** is a resident and citizen of the State of Louisiana. On or about early 2015, Plaintiff bought a Windows desktop which featured an Intel Pentium 3825U as the computer's CPU. Plaintiff bought the desktop online from HSN.com. Plaintiff reviewed and relied on the information about the desktop and Intel processor that was displayed HSN.com. Plaintiff purchased, and still owns, this device containing an Intel processor. Plaintiff read and heard

that Intel was an industry leader whose processors were the world's fastest and consistently outperformed competitors. Plaintiff was made aware of these claims via commercials she had seen on TV and online advertisements on websites she frequented on her mobile device. Plaintiff expected the processor to function as Intel advertised and represented. Implicit in Intel's representations was that its processor would deliver such performance securely, so that that data would not potentially be exposed to compromise. Any reasonable consumer would expect that the computing device being purchased would be secure and free from potential exploits.

53. Plaintiff has used (and continues to use) the Intel device to shop online, pay bills, schedule medication delivery, and make Skype video calls. She has also used the device to listen to gospel music, both online and on CD. Plaintiff has also used the desktop's disc drive to watch video DVDs. Plaintiff would and will frequently multitask while using the computer. Oftentimes, she would and will listen to gospel music while performing other tasks on the device. Moreover, Plaintiff rarely uses the device's web browser on only one task. Instead, multiple tabs remain open, one for online shopping and another for tracking bill payments, as plaintiff alternates between the two. Plaintiff's computer receives periodic updates that include the CPU patches released to date.

54. Unknown to Plaintiff, at the time of its purchase, the desktop was equipped with an Intel processor that contained undisclosed design Defects that made information, which should have remained secure and inaccessible, accessible to unauthorized parties. While security patches were implemented to protect against the Intel CPU Exploits, after January 2018 when the patches were downloaded, Plaintiff experienced material performance degradation, including reduced processing speed. Specifically, Plaintiff has experienced unexpected freezes and difficulty starting. In addition, as a result of the Defects in Intel's CPUs and Intel's mitigations needed to address the Intel CPU Exploits, Plaintiff spent time and effort researching the Intel CPU Exploits and implementing

available mitigations on her Intel device and purchased antivirus software to protect against malicious actors. Plaintiff currently experiences such significantly reduced processing speed that she usually uses her phone for tasks, when possible.

55. Plaintiff paid for processor performance that she did not receive.

56. Intel's unfair, unlawful, and deceptive conduct in designing, manufacturing, marketing, and selling its processors with the undisclosed Defects has diminished the value of Plaintiff's Intel processor and Plaintiff did not receive the benefit of the bargain. After disclosure of the Intel CPU Exploits, it became well known in the market that processor performance of Intel's CPUs would be negatively impacted—across the board—as a result of the necessary patches to secure data from the Intel CPU Exploits due to the undisclosed Defects in the CPUs. Plaintiff's Intel CPU is worth less than what she paid for it.

57. Plaintiff purchased a device containing the Intel processor on the reasonable, but mistaken, belief that the processor would provide the performance promised, would do so securely, and would retain all of its operating characteristics throughout its useful life. Had disclosures of the Defects in the Intel CPU's, or that mitigations needed to address the Intel CPU Exploits would materially impact the CPU's functionality and performance, been displayed online or in the store, Plaintiff would have seen them and no doubt have taken them into account in making her purchasing decision. In particular, had Plaintiff known about the Defects in Intel's CPUs or that mitigations needed to address the Intel CPU Exploits would materially impact the CPUs' functionality and performance, she would not have bought the desktop containing the Intel processor or would have paid less for it. Plaintiff would have purchased a desktop containing an AMD or other competing processor (which are reportedly immune from the Intel CPU Exploits) or paid only for a device with

a CPU delivering the diminished post-mitigation performance (not the promised pre-mitigation performance).

58. **Plaintiff Michael Nelson** is a resident and citizen of the State of Washington. On or about September 1, 2010, Plaintiff bought a new Windows desktop which featured an Intel Core i5-650 as the computer's CPU. Plaintiff bought the desktop from Best Buy in the store. Plaintiff reviewed and relied on the information about the desktop and Intel processor that was displayed. Plaintiff purchased, and still owns, this device containing an Intel processor. Plaintiff has heard and/or read that Intel processors were the world's fastest processors, had advanced performance, and were the industry performance leader. Plaintiff expected the processor to function as Intel advertised and represented. Implicit in Intel's representations was that its processor would deliver such performance securely, so that that data would not potentially be exposed to compromise. Any reasonable consumer would expect that the computing device being purchased would be secure and free from potential exploits.

59. Plaintiff has used (and continues to use) the Intel device for personal use and for his work as a college professor. Plaintiff multitasks on the computer, frequently running multiple applications at the same time. These include browsing the internet, using iTunes, editing photographs, word processing, creating spreadsheets, communicating with people through Skype and Zoom, and creating PowerPoint presentations. Plaintiff's computer receives periodic updates that include the CPU patches released to date.

60. Unknown to Plaintiff, at the time of its purchase, the desktop was equipped with an Intel processor that contained undisclosed design Defects that made information, which should have remained secure and inaccessible, accessible to unauthorized parties. While security patches were implemented to protect against the Intel CPU Exploits, after January 2018 when the patches were

downloaded, Plaintiff experienced material performance degradation, including reduced processing speed. Specifically, Plaintiff has experienced sluggish performance, and freezing of his computer while browsing the internet, requiring restarting. In addition, as a result of the Defects in Intel's CPUs and Intel's mitigations needed to address the Intel CPU Exploits, Plaintiff spent time and effort researching the Intel CPU Exploits and implementing available mitigations on his Intel device.

61. Plaintiff paid for processor performance that he did not receive.

62. Intel's unfair, unlawful, and deceptive conduct in designing, manufacturing, marketing, and selling its processors with the undisclosed Defects has diminished the value of Plaintiff's Intel processor and Plaintiff did not receive the benefit of the bargain. After disclosure of the Intel CPU Exploits, it became well known in the market that processor performance of Intel's CPUs would be negatively impacted—across the board—as a result of the necessary patches to secure data from the Intel CPU Exploits due to the undisclosed Defects in the CPUs. Plaintiff's Intel CPU is worth less than what he paid for it.

63. Plaintiff purchased a device containing the Intel processor on the reasonable, but mistaken, belief that the processor would provide the performance promised, would do so securely, and would retain all of its operating characteristics throughout its useful life. Had disclosures of the Defects in the Intel CPU's, or that mitigations needed to address the Intel CPU Exploits would materially impact the CPU's functionality and performance, been displayed in the store, Plaintiff would have seen them and no doubt have taken them into account in making his purchasing decision. In particular, had Plaintiff known about the Defects in Intel's CPUs or that mitigations needed to address the Intel CPU Exploits would materially impact the CPUs' functionality and performance, he would not have bought the desktop containing the Intel processor or would have paid less for it. Plaintiff would have purchased a desktop containing an AMD or other competing processor (which

are reportedly immune from the Intel CPU Exploits) or paid only for a device with a CPU delivering the diminished post-mitigation performance (not the promised pre-mitigation performance).

64. Defendant Intel Corporation is a Delaware corporation with its principal place of business located at 2200 Mission College Blvd., Santa Clara, California. At all relevant times, Intel designed, manufactured, distributed, marketed, and sold the defective CPUs throughout the United States.

CHOICE OF LAW

65. The application of California law to this litigation is appropriate given Intel's connection to the State of California since the 1970s. As Intel itself states:

> We purchased our first piece of property—a 26-acre pear orchard on the corner of Coffin Road and Central Expressway in Santa Clara, California in 1970. Today, we have 15,000 employees across the state at three major sites in Santa Clara, San Jose, and Folsom, and at research and development sites in Irvine and San Diego. Santa Clara is home to Intel's corporate headquarters and the flagship Intel Museum, which showcases five decades of Intel® innovations.[11]

66. Intel boasts that it has "invested in California for five decades, since our founding in Mountain View in 1968."[12]

67. But Intel's connection to California does not end in Santa Clara. It has divisions throughout the State of California, including in Folsom.

68. Intel states that its "Folsom site is a center of excellence for graphics, chipsets and solid state drives, delivering innovative technology and support for a wide range of devices and

[11] Intel in California, https://www.intel.com/content/www/us/en/corporate-responsibility/intel-in-california.html (as published Aug, 21, 2018).

[12] *Id.*

client platforms. With close to 6,000 employees, Intel is Folsom's largest private sector employer, and one of the Sacramento region's top 5 private employers."[13]

69. Intel's Santa Clara site, however, is where the fraudulent conduct as described herein originated. As Intel states, "The Santa Clara site is involved in engineering, design, research and development, and software engineering, and houses several corporate organizations, including sales and marketing, legal, supply chain, and human resources. With more than 6,500 employees, Intel is one of the largest employers in Santa Clara."[14]

70. Intel's own website even shows that nearly all of its available marketing jobs in the United States—the very arm of the Company that would have been responsible for the consumer-facing advertisements, representations, and even omissions—are located in the State of California.[15]

71. The State of California has a substantial interest in ensuring that corporations do not misrepresent their products, omit security risks concerning those products, and otherwise engage in business decisions that would harm consumers.

72. The application of California law to Intel—a California company that took substantial actions in the State of California impacting Plaintiffs and the Class members in the State of California—would be neither unfair nor unlawful; nor would it violate the Due Process Clause of the Fifth and Fourteenth Amendments to the U.S. Constitution.

---

[13] *Id.*

[14] *Id.*

[15] Intel Job Openings for "Marketing" Positions, https://jobs.intel.com/ListJobs/All/Search/jobtitle/marketing/ (as published Aug. 21, 2018).

SUBSTANTIVE ALLEGATIONS

A. General Background

1. Intel's 8086 and x86 Instruction Set

73. Intel, a portmanteau of the words "integrated" and "electronics," was founded by Robert Noyce and Gordon Moore in 1968 for the purpose of designing and manufacturing memory devices for computers utilizing silicon, a semiconducting material and one of the common elements found on Earth. In 1971, the Company went public and its shares have been traded on the NASDAQ continuously ever since. That same year, Intel launched the first commercially available microprocessor, the Intel 4004.

74. A microprocessor is an integrated electronic circuit that contains all the functions of a CPU of a computer. The CPU is the "brains" of the computing device, performing all necessary computations for each application (e.g., Microsoft Word) and each peripheral (e.g., a printer). Each program communicates with the processor through instructions, with each instruction representing a calculation or operation that the CPU must execute on behalf of the requesting application. For each calculation, the CPU "fetches" the instruction from the computer's memory, "decodes" it, "executes" it, and, finally, "writes-back" the result. The time it takes a CPU to process instructions is measured in "clock cycles." Each step in the process—fetch, decode, execute, and write-back—takes at least one clock cycle. The number of clock cycles a CPU completes per second is known as the "clock rate." "Clock speed" or "frequency" is a way to measure a CPU's processing speed and is usually expressed in megahertz ("MHz") or gigahertz ("GHz").

75. In 1978, Intel debuted the 8086 microprocessor. The 8086 was a 5 Mhz, 16-bit processor, capable of handling up to 1 megabyte ("MB") of data.[16] For the 8086, Intel designed an "instruction set," known as x86, and a "microarchitecture," known as 8086. The instruction set serves as an interface between a computer's software and hardware. The microarchitecture governs the various parts of the processor and how they work together to implement the instruction set.

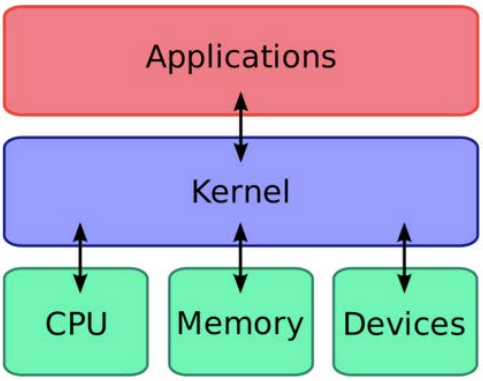
76. In July 1981, IBM launched its first personal computer ("PC"), powered by Intel's 8088 microprocessor, a more economical version of the 8086 microprocessor, also based on the x86 instruction set. Because IBM allowed Original Equipment Manufacturers ("OEMs"; that is computer manufacturers) to clone its PC design, IBM PCs and clones thereof soon dominated the market. Each of these computers was powered by a processor that implemented Intel's x86 instruction set. Today, the majority of all PCs, laptops, workstations, and servers are powered by processors based on Intel's x86 instruction set.

2. Intel's 80286 and the Introduction of Protected Mode

77. In 1982, Intel released its second-generation processor based on the x86 instruction set, the 80286. Before the 80286, processors had one operation mode known as "real mode." When the computer operated in real mode, applications had unlimited and direct access to all of a computer's memory, including information stored in the "kernel."

78. The kernel is the central part of the computer's operating system ("OS"). Notable OSs include Microsoft Windows, Linux, and Apple's MacOS. As demonstrated in the graphic below, the kernel acts as the intermediary between the CPU, memory, and any applications or peripherals:

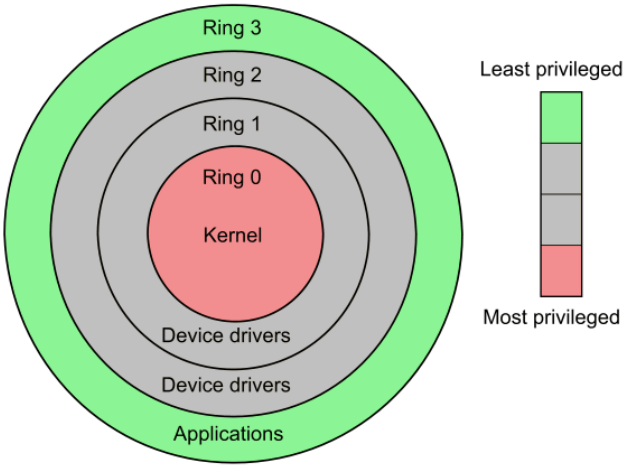
[16] A "bit" is the smallest unit of storage. A "byte" is equal to 8 bits.



79. When a computer is operating in real mode, it is possible for a malfunctioning or malignant application to access the kernel and overwrite the OS, leading to catastrophic failure of the computer. Today, such a failure could lead to "kernel panic" or, on a computer running Windows, the feared "Blue Screen of Death," which is displayed if the OS experiences a fatal system error.

80. In order to minimize OS failures, Intel's 80286 introduced the concepts of "protected mode" and "virtual memory." Protected mode allows the OS to remain in control of the computer through the kernel. "Virtual memory" allows the computer to segment its physical memory into separate spaces, including "kernel space," where the computer runs and stores the critical kernel code, and "user space," where the computer runs and stores all of the other code needed to run the applications and peripherals.

81. The relevant importance of the code is determined by utilizing the concept of "protection rings." As demonstrated in the graphic below, "Ring 0" includes the most privileged information, which resides in the kernel, while "Ring 3," includes the least privileged information, which is accessible to virtually all applications:

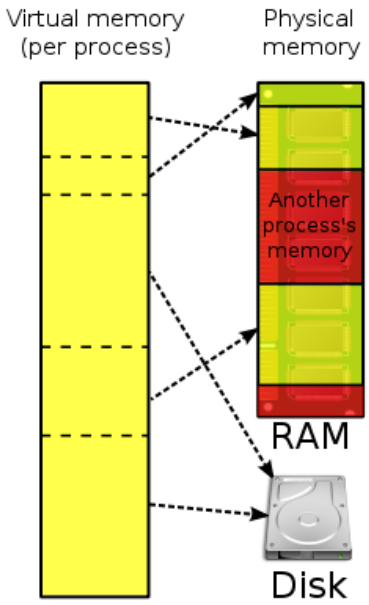


82. Access to these spaces is controlled by a program's "privilege level." To protect the computer's most privileged information (Ring 0), engineers rely on the "principle of least privilege," meaning that every program only has access to the least amount of privileged information it needs to perform its intended function. Typically, before a CPU fetches instructions or data requested by an application, the computer must first determine whether that program has the requisite privilege level to access that information. If the application does not have permission to access the requested instructions or data, an exception occurs within the CPU and the request fails.

83. The privilege levels defined in the x86 instruction set are meant to ensure that programs other than the kernel do not have direct access to a computer's most privileged information and that, if access is required, it is controlled by and is initiated through the kernel. This ensures that no application can access a computer's Ring 0 information or make changes to the OS without involving the kernel.

84. With the launch of the 80386 processor in October 1985, the functionality of protected mode and virtual memory was improved, and to this day all modern processors utilize these functionalities to protect a computer's most privileged information.[17]

85. With virtual memory, each user process has its own virtual address space, which creates the illusion that each user has a memory space much larger than the physical, hardware-backed memory actually available on the machine. In fact, user processes are sharing the limited physical memory, and portions of each program's instructions or data may actually be located in secondary storage (e.g., on disk).



86. The virtual address space allows each program to believe it is the only one (aside from the kernel (OS)) that is running on the machine. This serves as a security function by isolating processes from each other, and also helps prevent applications from. User applications should not be able to access each other's memory, or read or write to kernel memory, without permission. This

[17] Michael S. Malone, *The Intel Trinity: How Robert Noyce, Gordon Moore, and Andy Grove Built the World's Most Important Company* (2014).

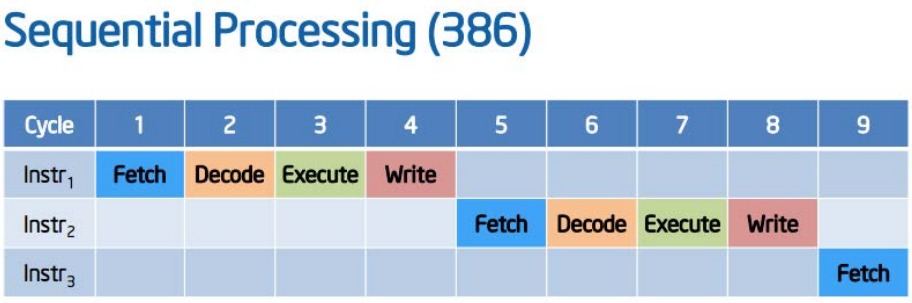
allows multiple applications to run simultaneously on personal devices and multiple users to execute processes on the same machine in the cloud.

87. When a processor seeks to access data or instructions from memory, a virtual address has to be translated into a physical address to determine where the information is located. Page tables are used to map the virtual to physical addresses, translating the virtual addresses seen by an application into physical addresses used by the hardware.

3. Intel's 80486 and the Introduction of Pipelines and On-Die Caches

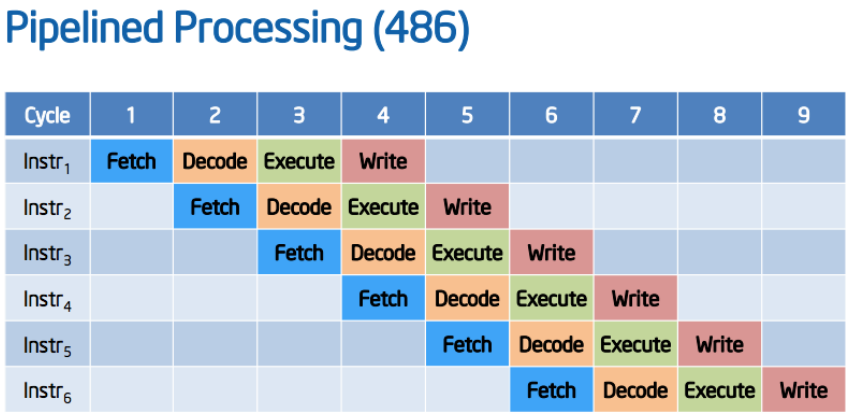
88. Intel introduced the next generation of the x86-based processor, the 80486, in 1989. The 80846 boasted twice the performance of the 80386, due in part to two key improvements to the microarchitecture: pipelines and on-die caches.[18]

89. **Instruction Pipelining.** Earlier iterations of Intel's x86-based processors utilized "sequential" processing, working through each step of the first instruction (e.g., fetch, decode, execute, and write-back) before starting the next instruction. The following diagram reflects the 80386's sequential processing. In this example, it takes eight clock cycles to complete two instructions:

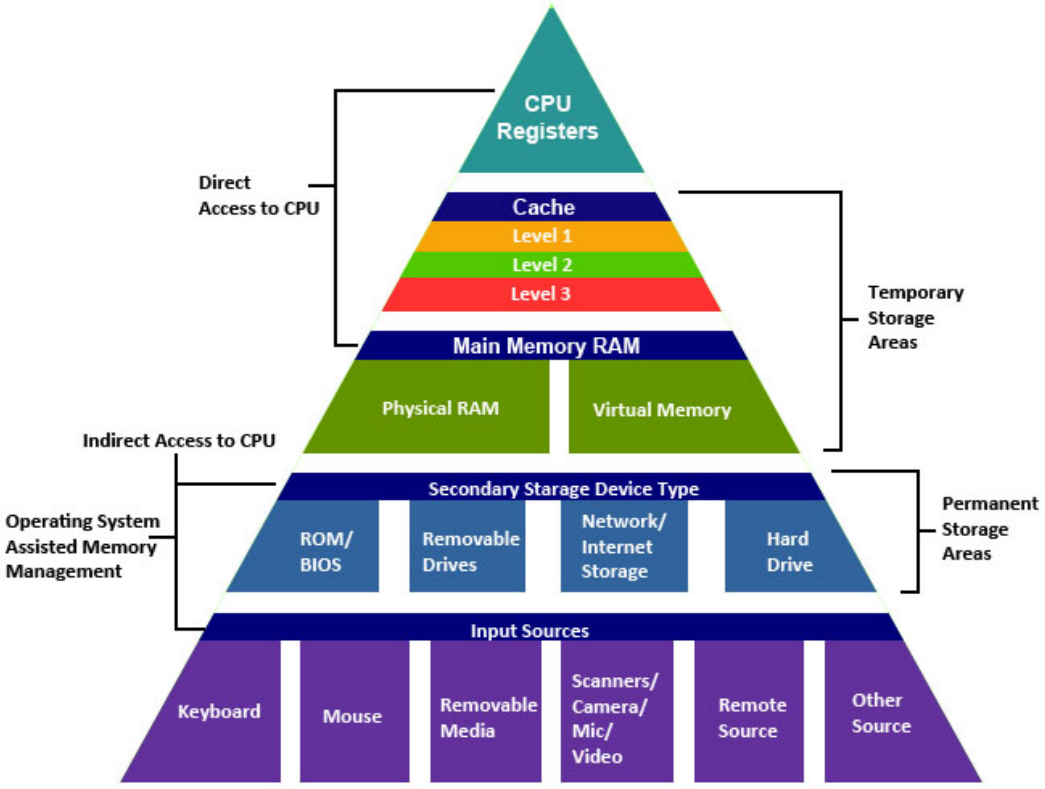


[18] Michael S. Malone, *The Intel Trinity: How Robert Noyce, Gordon Moore, and Andy Grove Built the World's Most Important Company* (2014).

90. The 80486 was a "pipelined" processor, meaning that the CPU began processing the next instruction before it had completed processing the prior instruction. As reflected in the diagram below, on Clock Cycle 2, the 80486 was able both to decode the instruction fetched during Clock Cycle 1, and to concurrently fetch the next instruction. With pipelining, the 80486 could complete six instructions in nine clock cycles, nearly tripling the work completed in the same amount of time:



91. **Memory Hierarchy and On-Die Caches.** A computer's memory system, which holds instructions and data for the CPU, is a hierarchy of storage devices with different capacities and access times. When the CPU needs instructions or data to complete a task, it must fetch it from memory. The following pyramid helps depict the basic memory hierarchy:



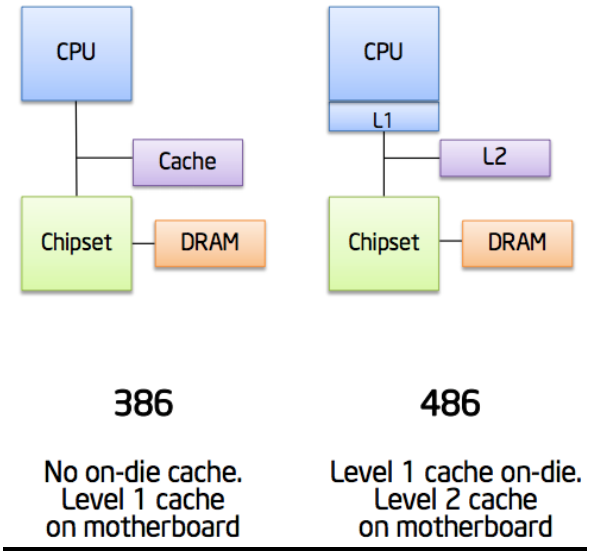
92. Data in the CPU registers can be operated on immediately during execution by the CPU.

93. A computer's physical memory space—known as "main memory"—is separated from the CPU on the computer's main circuit board or motherboard. Fetching instructions or data from main memory is highly inefficient because main memory runs at a slower speed than the CPU (the "performance gap") and because of the time it takes for information and data to travel between main memory and the CPU on the motherboard ("latency").

94. In order to lessen the performance gap and the issue of latency, modern microarchitecture designs rely on caches. A "cache" is a location between main memory and the CPU that can be used to temporarily store information and data for the use of the CPU. Caches typically operate at the same or similar speed as the CPU, shrinking the performance gap. Caches

also are located in closer proximity to the CPU, addressing the latency problem. As a result, when a processor needs to fetch instructions or data, it can first check to see if the necessary information has been stored in the cache. If the information is in the cache (a "cache hit"), the CPU avoids the delay and associated performance penalty associated with fetching the information from main memory. If the information is not in the cache (a "cache miss"), the CPU fetches it from main memory.[19]

95. Because caches help minimize delays associated with fetching information from main memory, a processor with at least one cache typically is faster than a processor without any caches. While prior generations of Intel's x86-based processors included a first level or "L1" cache between main memory (referred to as "DRAM" in the diagram below) and the CPU on the motherboard, the 80486 brought the L1 cache onto the same "die" (or piece of silicon) as the CPU and added a separate second level or "L2" cache to the motherboard:



[19] Worse yet, if not present in main memory, the data or instructions must be fetched from storage, e.g., disk, which is even slower.

96. By placing the L1 cache directly on the CPU die, the 80486 further decreased the time needed to fetch instructions and data, improving latency. By adding a second cache (L2), the increased overall cache capacity made it more likely the CPU would find the information it needed in one of the caches, without having to resort to fetching it from main memory.

97. Despite the 80486's clear performance advantage, however, Intel struggled to convince OEMs to launch PCs powered by the 80486 or to convince end-users that they needed one.

98. To make matters worse, at the end of 1990, Intel's largest competitor, AMD launched a clone of Intel's 80386 microprocessor, the AM386, which was faster and cheaper than Intel's 80386. Notably, this was not the first time that AMD had launched a faster clone of an Intel processor. With the 80286, IBM required Intel to use AMD as a second supply source, effectively forcing Intel to give to its competitor a license to the 80286 code. This was not a good development for Intel: AMD's 80286 clone, the AM286, could run as fast as 25 MHz, while Intel's 80286 processors clocked between 6 MHz and 12 MHz.[20] As a result, when Intel subsequently launched the 80386, the Company refused to grant AMD a license.

99. In response to the success (and speed) of the AM386, Intel sued AMD and launched a $250 million multi-media "Intel Inside"-based campaign to push the end-users to demand from the OEMs PCs powered by Intel's new 80486 microprocessor. Intel had started its "Intel Inside" campaign in 1989 by asking PC makers, including IBM, to place "Intel Inside" stickers on the computers themselves to generate brand-loyalty among the end-users.[21] The goal of the campaign

[20] Michael S. Malone, *The Intel Trinity: How Robert Noyce, Gordon Moore, and Andy Grove Built the World's Most Important Company* (2014).

[21] *Intel Launches a Huge Advertising Campaign: *Technology: The $250-million blitz is aimed at cutting down the competition and selling its next-generation 486 microprocessors*, Los Angeles

was to cultivate in consumers the belief as to the reliability and superior performance of Intel-branded processors and to ensure that they could differentiate between an Intel processor and a clone made by one of its competitors. As Intel's former CEO, Andrew Grove described it, "Intel Inside" drove home the point "that the identity and class of the computer were determined more than anything else by the microprocessor within."[22]

100. The campaign worked. Not only did customer pressure lead to OEMs announcing new PCs powered by Intel's 80486, but many of the manufacturers agreed to use the "Intel Inside" branding in their own marketing efforts. By 1997, 1,500 OEMs were incorporating the "Intel Inside" theme into their marketing efforts.[23] By 2000, Intel was the second-best-known industrial brand (after Coca-Cola) in the world.[24]

4. Intel's P5 Microarchitecture

101. In 1993, Intel introduced its fifth-generation microarchitecture based on the x86 instruction set, known as P5. Intel launched the "Pentium"-branded processors based on P5.

102. The P5-based processors were significantly faster due to their superscalar design. Whereas pipelining allowed a CPU to process different aspects of multiple instructions at the same time, a superscalar design allowed the CPU to fetch two instructions at the same time, decode two instructions at the same time, and so forth. A pipelined superscalar design, such as the P5-based

---

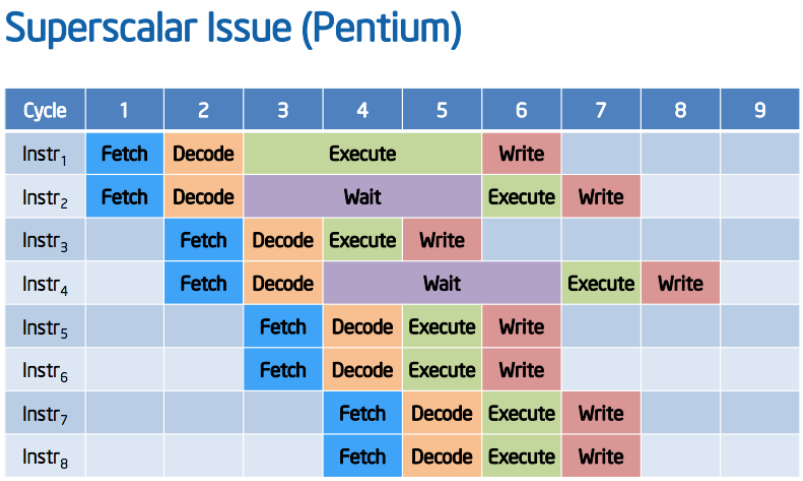
Times (Nov. 2, 1991), http://articles.latimes.com/1991-11-02/business/fi-797_1_advertising-campaign.

[22] Andrew S. Grove, *Only the Paranoid Survive: How to Exploit the Crisis Points That Challenge Every Company* (1988).

[23] *Intel Corp.*, AdAge Encyclopedia (Sept. 15, 2013), http://adage.com/article/adage-encyclopedia/intel-corp/98721/.

[24] Michael S. Malone, *The Intel Trinity: How Robert Noyce, Gordon Moore, and Andy Grove Built the World's Most Important Company* (2014).

Pentium processor, allowed the processor to decode Instructions 1 and 2, while fetching Instructions 3 and 4:



103. As compared to a sequential processor (e.g., the 80386 at two instructions in eight clock cycles), and a pipelined processor (e.g., the 80486 at six instructions in nine clock cycles), a superscalar pipelined processor could complete eight instructions in eight clock cycles.

104. Intel used its "Intel Inside" campaign to make "Pentium" a household name. The success of the campaign, however, became a curse once Intel discovered, in the summer of 1994, that Pentium had a design flaw. Intel initially decided not to publicly disclose the defect because it believed very few customers would be impacted. The flaw, though, was later uncovered by a North Carolina professor in October 1994, ultimately leading to intense media scrutiny. The *Wall Street Journal*'s principal technology columnist, Walter Mossberg, described the scandal as worse than Watergate. IBM, in turn, suspended shipment of all Pentium-powered PCs on December 12, 1994, because its independent research confirmed the flaw was more serious than Intel had represented.[25]

[25] *Id.*

105. At first, Intel resisted public pressure to conduct a full recall, continuing to sell the flawed Pentium and agreeing only to issue replacements if consumers could demonstrate that they were likely to encounter the flaw. On December 19, 1994, however, just one week after IBM suspended shipments of Pentium-powered PCs, Intel finally agreed to a full recall. On January 17, 1995, Intel announced that it would spend $475 million to replace the flawed processors and that, going forward, that it would immediately disclose any and all defects in its future microprocessors.[26]

5. Intel's P6 and the Introduction of Dynamic Execution

106. Intel introduced its P6 architecture in November 1995. Makers of large computers, servers, and workstations quickly embraced the P6-based Pentium Pro processors.[27] In 1997, Intel also successfully launched the Pentium II processor, a more consumer-oriented processor based on the P6 architecture.

107. In a number of ways, the P6 microarchitecture represented a break from Intel's prior x86-based designs. As explained by Intel on its launch, the P6 "microarchitecture was tuned to what was proven performance," "[o]ptimizing CPI [clock per instruction] and [f]requency" to achieve a "50% frequency gain," and, ultimately, a "37% performance gain." In designing the P6 microarchitecture, Intel determined that "Dynamic Execution," which included the concepts of "out-of-order execution," "speculative execution," and "branch prediction" was "required for higher performance."[28]

---

[26] *Id.*

[27] *Id.*

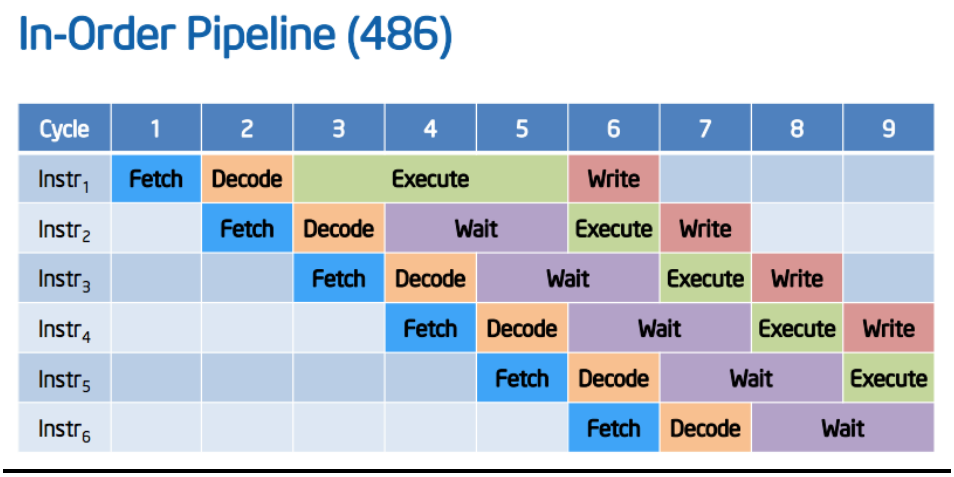
[28] David Papworth, *Optimizing the P6 Pipeline*, Presentation at 1995 Hot Chips Conference, https://www.hotchips.org/wp-content/uploads/hc_archives/hc07/2_Mon/HC7.S2/HC7.2.1.pdf.

108. **Out-of-Order Execution.** Every application or program has a set of instructions that it wants the CPU to execute in order ("program order"). These instructions require the CPU to, for example, engage in arithmetic or logical functions.

109. Instructions can be "data dependent," meaning that the instruction needs the data produced by a preceding instruction in order to execute. For example, suppose the CPU needs to add four numbers together: 1, 32, 75, and 89. Instruction 1 can add the first two numbers (1+32=33) and Instruction 2 can add the second two numbers (75+89=164). Instruction 3, however, is a data dependent instruction because the CPU needs the results of Instruction 1 (33) and Instruction 2 (164) to execute it.

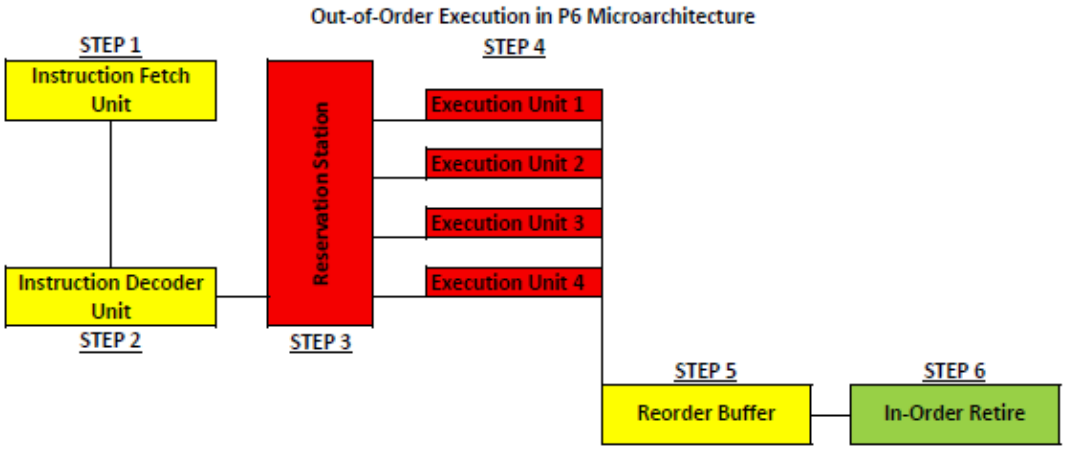
110. Instructions also can be "conditional" expressed as, "if X, then Y." For instance, Microsoft Word has an autocorrect feature that determines whether a word is spelled correctly after it is typed. If the word is spelled incorrectly, the program fixes it. In that scenario, the conditional instruction is, "If a word is misspelled (X), then fix it (Y)." With Word's autocorrect feature, there are two possibilities or "branches"—there is a misspelling that needs to be fixed, or there is no misspelling and the CPU can move on to another instruction. A conditional instruction has to be resolved before the CPU can determine the next step or branch to take. For this reason, such conditional instructions are sometimes called "branch instructions."

111. Data dependent and conditional instructions (among others) can take a number of clock cycles to execute, leading the CPU to "stall" while it waits for the necessary data or branch it should follow to execute the next instruction. The diagram below shows "in-order" execution in an 80486 pipelined processor where the CPU is stalled with respect to Instructions 2-6. When Instruction 1 takes six clock cycles, only three instructions are complete at the end of eight clock cycles, as compared to five instructions after eight clock cycles where there is no CPU stall.

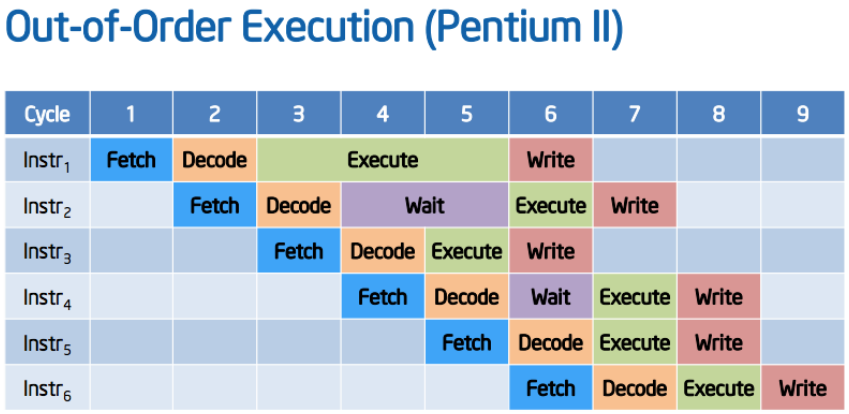


112. Out-of-order execution ("OoOE") addresses this problem. Instead of executing each instruction in "program order," the CPU executes instructions based on "dataflow order," or, in other words, the CPU executes instructions based on an order determined by what data is available to it at any given time. Dataflow order is akin to what students are taught to do with standardized tests—complete questions for which the answer is known first, before going back to those questions for which the answer is not immediately clear.

113. The following diagram shows OoOE in the P6 microarchitecture. In Steps 1 and 2, the instructions are fetched, decoded, and moved to the Reservation Station. In Step 3, the Reservation Station sends instructions in dataflow order to the Execution Units. During Step 4, the Execution Units execute the instructions and send the results to the Reorder Buffer. Information necessary to execute these instructions is held in the processor's cache. The Reorder Buffer puts the instructions back into "program order" (Step 5) and sends them to be retired in order (Step 6).



114. With OoOE, P6-based processors can overcome the CPU stall generated by Instruction 1 in the image below and execute five instructions in eight clock cycles, eliminating the performance penalty and speeding up the processor.

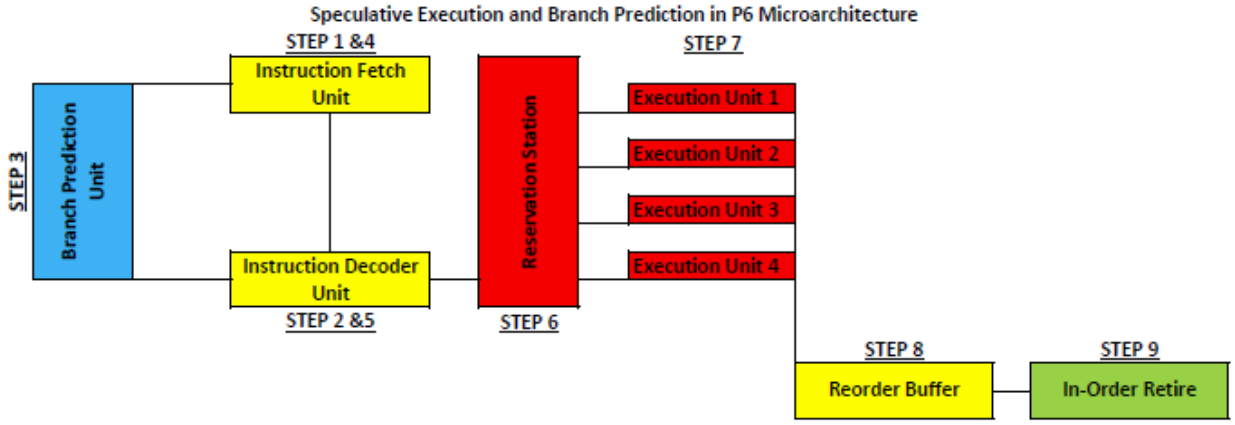


115. Ultimately, Intel concluded that OoOE was helpful because it "allowed higher clock frequency without CPI [average clock cycles per instruction] degradation" and "provid[ed] more performance per square mil of datapath."[29]

[29] David Papworth, *Optimizing the P6 Pipeline*, Presentation at 1995 Hot Chips Conference, https://www.hotchips.org/wp-content/uploads/hc_archives/hc07/2_Mon/HC7.S2/HC7.2.1.pdf.

116. **Branch Prediction and Speculative Execution.** While OoOE improves the performance of a processor by mitigating CPU stalls generated by data dependent instructions, only branch prediction and speculative execution ameliorate the performance impact of conditional instructions on the CPU. When the CPU fetches and decodes a conditional instruction, the processor predicts the "branch" based on prior results and then speculatively executes instructions down that branch until the conditional instruction is executed and the branch is resolved.

117. The following diagram demonstrates branch prediction and speculative execution in the P6 microarchitecture. If a conditional instruction is fetched and decoded (Steps 1 and 2), then the Branch Prediction Unit (Step 3) is queried, with the resulting guess going to the Instruction Fetch Unit in Step 4. From there, the processor decodes and speculatively executes the instructions down the predicted branch (Steps 5-7). Meanwhile, the information for these speculatively executed instructions is stored in the processor's caches.



118. When the CPU eventually executes the conditional instruction, the processor checks whether its prediction was correct. If the Branch Prediction Unit has guessed correctly, the processor has performed useful work and the results are written to memory (Step 9, above). If the CPU has guessed incorrectly—a "mispredicted branch"—the processor "flushes" its pipeline of the

impact of the speculatively executed instructions and proceeds to execute the instructions from the correct path. Critically, and as further explained in Section B, according to Intel's microarchitecture design, the CPU does not flush its cache after a mispredicted branch and so the information associated with the speculative execution down the incorrect branch remains in the processor.

119. Research shows that Intel's P6 architecture did not permit unauthorized access by programs to protected memory. In other words, the P6 did not implement the Unauthorized Access Defect to allow instructions to access the read value (and instead returned a random number similar to AMD's CPUs).[30]

6. The Netburst Microarchitecture Disaster

120. The speed at which a CPU performs is a material attribute for consumers purchasing a desktop, laptop, workstation, or server powered by an Intel processor. Without sufficient processing speed, a CPU will be unable to effectively and efficiently run the device's OS and applications, or to utilize connected hardware and peripherals. As a result of Intel's various direct-to-consumer marketing campaigns, including "Intel Inside," consumers look to and rely upon the processor's advertised clock speed to measure a CPU's performance. Intel's focus on clock speed in its marketing led to the "Megahertz Wars," followed by the "Gigahertz Wars," during which Intel and its main competitor, AMD, battled to see which company could achieve the fastest clock speed.

121. After successfully cloning the 80286, 80386, and 80486, AMD launched its own x86-based microarchitecture design, K5, in 1995. Like Intel's P6, AMD's microarchitecture designs relied upon OoOE, speculative execution, and branch prediction to achieve performance increases

[30] *See* H. Wong, *The Microarchitecture Behind Meltdown*, StuffedCow.net (May 18, 2018), http://blog.stuffedcow.net/2018/05/MELTDOWN-MICROARCHITECTURE/

over earlier generations of processors. In July 1999, AMD took the "speed crown" from Intel with the launch of its K7-based Athlon-branded processors.[31] Thereafter, the title of the fastest processor changed hands several times.

122. Then in March 2000, AMD successfully launched the first processor that could reach 1 GHz. Desperate to also reach the coveted goal of 1 GHz, Intel resorted to introducing the 1 GHz P6-based Pentium III processor just two days later, well before the Company was ready to ship these processors, as well as the previously announced 850, 866, and 933 MHz P6-based Pentium III processors to consumers. Intel quickly followed this much-derided "paper launch" by announcing a 1.13 GHz Pentium III processor in July 2000.[32]

123. Problems, however, with the 1.13 GHz Pentium III on the test bench led tech reviewers to publicly conclude that Intel had serious production issues with its 1.13 GHz CPU. After a third outlet, *AnandTech*, came forward, confirming these reports, Intel recalled the 1.13 GHz Pentium III in August 2000, approximately one week after the first shipments of these processors had reached customers.

124. Hoping to outrun the negative press that it had generated over the last year, Intel announced its newest microarchitecture, Netburst and Netburst-based Pentium 4 processors in November 2000. According to Intel, Netburst-based CPUs "feature[d] significantly higher clock rates and world-class performance."

125. Although the original Pentium 4 processors clocked at just over 1 GHz, Intel designed the Netburst microarchitecture with room to allow successive processors to reach clock

[31] Anand L. Shimpi, *Intel's 1.13GHz CPU Recalled_Is Intel resorting to desperate measures?*, AnandTech (Aug. 29, 2000), https://www.anandtech.com/show/613/2

[32] *Id.*

speeds of up to 10 GHz. To reach these speeds, Netburst included an improved cache subsystem, featuring larger, faster caches, a deeply pipelined design (doubling the number of pipeline stages), and "hyper-threading" technology, to ensure that the CPU was effectively and efficiently taking advantage of all available resources to achieve increased frequency and performance benchmarks.

126. Intel designed the first Netburst-based processors, Pentium 4s code-named "Willamette," to reach clock speeds of 1.5 GHz. The Willamette processors, though, could not outscore the P6-based Pentium IIIs or AMD's Athlon processors in commercially available benchmark testing. In a lawsuit filed in 2002 in California state court, styled *Skold v. Intel Corp.*, No. 1-05-CV-039231 ("*Skold*"), consumers who ultimately purchased computers powered by the Willamette processors alleged that the "Pentium 4's scores were so bad that Intel [internally] deemed it 'not competitive' with AMD's Athlon processor or . . . [the] Pentium III processor, noting that most benchmark tests showed a 'negative or zero performance gain.'"

127. According to the plaintiffs in *Skold*, the Willamette processors performed poorly due to "design flaws" in the Netburst architecture, which "Intel admitted . . . were so serious and so pervasive that they would significantly impair any computer's performance by dramatically slowing its ability to process the computer's instructions." These flaws were the result of "a 'complete failure' of the design process," requiring "a dramatic change in [Intel's] engineering" process and a redesign that would prevent Intel from releasing a new processor for another two years.

128. With AMD already taking market share, Intel could not wait until 2002 to launch a competitive processor. Through its "Intel Inside" campaign, the Company had conditioned consumers to look to computers containing Intel processors for superior performance and reliability. By focusing on processing speed and commercial benchmarking, Intel likewise had conditioned the market to focus on clock speed to measure a processor's performance and determine which

computer to purchase. Moreover, critically, Intel priced its processors based on the market's perception of their performance. In fact, Intel was able to garner a premium for its processors throughout the 1990s.

129. If, however, Intel released the Willamette processors, the public would soon learn what the Company already had discovered internally: the Pentium 4 was an overpriced dud. As reported in *Skold*, "Intel solved its problem by making it *appear* as if the [Willamette processor] outscored the Pentium III and AMD Athlon processors" (emphasis in original) by inflating its performance scores after it publicly launched the processor. This strategy included surreptitiously developing a new, purportedly independent benchmark and altering another purportedly independent benchmark to fool consumers into thinking that Intel's Willamette processor outperformed the Pentium III and AMD processors. Intel also disabled features on the Pentium III, hobbling its performance so that the Willamette processors would appear faster by comparison. OEMs like HP were incentivized to help Intel with its deception in order to sell more computers.

130. Ultimately, Intel settled the *Skold* lawsuit in 2014, agreeing to pay a 49-state class of consumers who had purchased a computer powered by a Willamette processor $15 per device.

7. Intel's Core Microarchitecture

131. After the Willamette debacle, Intel tried several times (without success) to release a number of processors based on the Netburst microarchitecture in response to AMD's successful products, including dual-core Athlon and Opteron processors. In a last-ditch attempt to make Netburst work, Intel designed, tested, and launched (in just nine months) "Smithfield," a dual-core, high-end Netburst-based processor. By August 2005, as reported by PCWorld, Intel publicly

admitted that its "first dual-core [processor] was a hastily concocted design that was rushed out the door in hopes of beating rival … [AMD] to the punch."[33]

132. The failed Smithfield launch made it clear that Intel had hit a wall. Where Intel was once able to announce materially increased clock speeds with each new processor, now it was lucky if it could eke out a single-digit percentage increase. Intel's designs could not handle the heat generated by higher clock speeds (the "thermal wall") or support the power necessary to materially increase clock speeds with each new processor (the "power wall"). The last Netburst-based processor, Prescott, never clocked higher than 3.8 GHz. As a result, Intel scrapped Netburst and designed its next microarchitecture, known as "Core," to achieve higher performance through more efficient design.

133. Released in 2006, Core rejected Netburst's reliance on a deeply pipelined, single-core processor, in favor of dual- or multi-core processors with cache subsystems. Work on Core started in 2001, after Intel had lost the speed crown to AMD and the initial failure of Netburst in the Willamette Pentium 4 processors.[34] Intel went back to its P6 microarchitecture design, and enlisted a team of engineers, who had designed the first microarchitecture for mobile computers (e.g., laptops), Pentium M, based on P6.[35]

134. Core-based processors relied on techniques, including OoOE, speculative execution, and branch prediction, to address stalls, misses, mispredictions, and other taxes on a processor's

[33] Tom Krazit, *First Dual-Core Pentium 4 a Rush Job, Intel Says*, PC World (Aug. 17, 2005), https://www.pcworld.com/article/122236/article.html.

[34] Glenn Hinton, *Key Nehalem Choices*, Intel Fellow Nehalem Lead Architect Presentation (Feb 17, 2010), https://www.slideshare.net/parallellabs/10intelnehalemdesignslides.

[35] Fedy Abi-Chahla, *Intel Core i7 (Nehalem): Architecture by AMD?*, Tom's Hardware, (Oct. 14, 2008), https://www.tomshardware.com/reviews/Intel-i7-nehalem-cpu,2041.html.

overall performance. On its release, Intel heralded Core as "a new foundation for Intel architecture-based desktop, mobile, and mainstream server multi-core processors," explaining that it had been "[d]esigned for efficiency and optimized performance across a range of market segments and power envelopes."

135. With Core, Intel expanded its use of Dynamic Execution (OoOE, speculative execution, and branch prediction) to enable delivery of more instructions per clock cycle. Intel designed each "core" or independent processing unit within the processor, often called a "processing element" or a "core," such that it could fetch, dispatch, execute, and retire up to four full instructions simultaneously. Intel increased the instruction buffers (similar to the Reservation Station in the P6 design) for greater execution flexibility.

136. Intel also attempted to enhance the Branch Prediction Unit. According to Intel, "branch prediction" is among the processors' functions that have "the greatest leverage for improving overall performance" because of the penalty associated with recovering from an incorrectly predicted branch. As Intel explained, "more efficient branch prediction gives better efficiency *with no other changes to the machine.*"[36]

137. Additionally, Core featured a redesigned memory and cache subsystems. With "Smart Memory Access," Intel purported to improve the processor's performance by more effectively utilizing the current system of buffers and cores to hide latencies created by accessing main memory. Intel also imbued each execution core with the ability to speculatively load data for

[36] *The Next Generation of Intel Core Microarchitecture*, Intel Technology Journal, Volume 14, Issue 3 (2010) https://www.intel.com/content/dam/www/public/us/en/documents/research/2010-vol14-iss-3-intel-technology-journal.pdf (emphasis in original). All quotes unless otherwise specified are from this source.

instructions prior to execution. With "Advanced Smart Cache," Intel created a large shared L2 cache accessible by both cores on a chip.

138. Intel's renewed reliance on Dynamic Execution, including branch prediction, and efficient memory and cache access led to reports of increased performance in processors based on the Core architecture. Core-based desktop and server processors boasted 40% and 80% increased performance, respectively, over similar processors based on Netburst.[37] Furthermore, these performance increases came at decreased clock speeds—the 2.66 GHz Core Duo 2 achieved 40% greater performance over a 3.6 GHz Netburst-based Pentium D processor.[38] With Core, Intel stabilized its market share[39] and won back the performance crown[40].

139. Unbeknown to Plaintiffs and members of the Class, however, research revealed that, unlike Intel's P6 architecture, Intel's Core architecture permitted unauthorized access by programs to protected memory. In other words, the Core architecture purposely implemented the Unauthorized Access Defect to allow instructions to access the read value (instead of returning a random number similar to Intel's P6 and AMD's CPUs).[41] Intel accomplished this in secret in order achieve superior performance over AMD's processors. Indeed, the Defects were consciously designed and implemented by Intel as undisclosed performance features.

---

[37] 2006 Intel Annual Meeting Slides.

[38] Jack Dowek, *Inside Intel Core Microarchitecture*, Intel, https://www.hotchips.org/wp-content/uploads/hc_archives/hc18/3_Tues/HC18.S9/HC18.S9T4.pdf (last visited May 5, 2020).

[39] 2006 Intel Annual Meeting Slides.

[40] [40] Fedy Abi-Chahla, *Intel Core i7 (Nehalem): Architecture by AMD?*, Tom's Hardware (Oct. 14, 2008), https://www.tomshardware.com/reviews/Intel-i7-nehalem-cpu,2041.html.

[41] *See* H. Wong, *The Microarchitecture Behind Meltdown*, Stuffedcow.net (May 18, 2018), http://blog.stuffedcow.net/2018/05/MELTDOWN-MICROARCHITECTURE/.

8. "Tick/Tock" and the Nehalem Architecture

140. Beginning with Core, Intel made "[p]erformance . . . an integral part of production definition and success." To that end, "Intel set[] very aggressive performance targets to deliver products with compelling performance to the end user."[42] Intel also "employ[ed] significant time and effort to ensure that the processor performance me[t] expectations at every stage of the product development cycle from concept to silicon arrival to product launch. All design decisions [we]re weighed against performance impact."

141. With the introduction of Core in 2006, Intel announced "an ambitious plan to return to evolving its processor architectures at a rapid pace, as [it] had done in the mid-1990s" known as "Tick-Tock."[43] Each "Tick" represented Intel's effort to optimize the current microarchitecture design for a new manufacturing process or, in other words, shrinking the processor to fit on a smaller piece of silicon. The first "Tick" after Core was the Penryn microarchitecture, which optimized Core for the 45-nanometer (nm) manufacturing process. Each "Tock" represented Intel's effort to redesign its microarchitecture. Under this product cycle, Intel utilized parallel design teams and committed to releasing either a Tick or a Tock each year.

142. The "starting point" for the first Tock following Core—known as Nehalem—was the previous Tick, the Penryn microarchitecture.[44] As Intel reported, with Penryn-based processors,

---

[42] *The Original 45-nm Intel Core 2 Processor Performance*, Intel Technology Journal, Volume 12, Issue 3 (Oct. 2008), https://www.intel.com/content/dam/www/public/us/en/documents/research/2008-vol12-iss-3-intel-technology-journal.pdf.

[43] Fedy Abi-Chahla, *Intel Core i7 (Nehalem): Architecture by AMD?*, Tom's Hardware (Oct. 14, 2008), https://www.tomshardware.com/reviews/Intel-i7-nehalem-cpu,2041.html.

[44] "The Next Generation of Intel Core Microarchitecture," Intel Technology Journal, Volume 14, Issue 3 (2010), The Next Generation of Intel Core Microarchitecture," Intel Technology Journal, Volume 14, Issue 3 (2010). All quotes unless otherwise specified are from this source.

"Intel delivered a product with record-breaking performance on a wide range of client and server applications" by implementing "[f]requency improvements," "a larger L2 cache," and other "microarchitectural enhancements."[45] With the Nehalem microarchitecture design Intel sought "a greater utilization of the possible peak performance" of the processor.

143. Work had begun on Nehalem in 2003. While most of the microarchitecture decisions were made in 2004, the major engineering work was done between 2005-07.[46] Because Intel was forced to get Core out the door quickly to stop the fallout from the Netburst fiasco, Core was not fully optimized for all types of processor use cases.[47] Whereas Core supported up to two cores, Nehalem was designed to effectively and efficiently support multiple cores and for use in laptops, desktops, and servers alike.[48] Or, as Intel told shareholders at its 2006 Annual Meeting, "One Micro-Architecture for all High Volume Segments."

144. To accomplish this, and eliminate a perceived "performance bottleneck," Intel implemented branch prediction in Nehalem's OoOE engine that sought to feed the engine "code and data at an unprecedented rate." As *Ars Technica* explained, "to imagine that the [Penryn-based processor's] thirsty execution engine has been separated from the pools of code and data that lay in main memory by relatively thin pipes (the frontside-bus and cache hierarchy)" by "replacing the

---

[45] *The Original 45-nm Intel Core 2 Processor Performance*," Intel Technology Journal, Volume 12, Issue 3 (Oct. 2008), https://www.intel.com/content/dam/www/public/us/en/documents/research/2008-vol12-iss-3-intel-technology-journal.pdf. All quotes in this section unless otherwise specified are from this source.

[46] Glenn Hinton, *Key Nehalem Choices*, Intel Fellow Nehalem Lead Architect Presentation (Feb 17, 2010), https://www.slideshare.net/parallellabs/10intelnehalemdesignslides..

[47] [47] Fedy Abi-Chahla, *Intel Core i7 (Nehalem): Architecture by AMD?*, Tom's Hardware (Oct. 14, 2008), https://www.tomshardware.com/reviews/Intel-i7-nehalem-cpu,2041.html.

[48] Glenn Hinton, *Key Nehalem Choices*, Glenn Hinton Intel Fellow Nehalem Lead Architect Presentation (Feb 17, 2010), https://www.slideshare.net/parallellabs/10intelnehalemdesignslides.

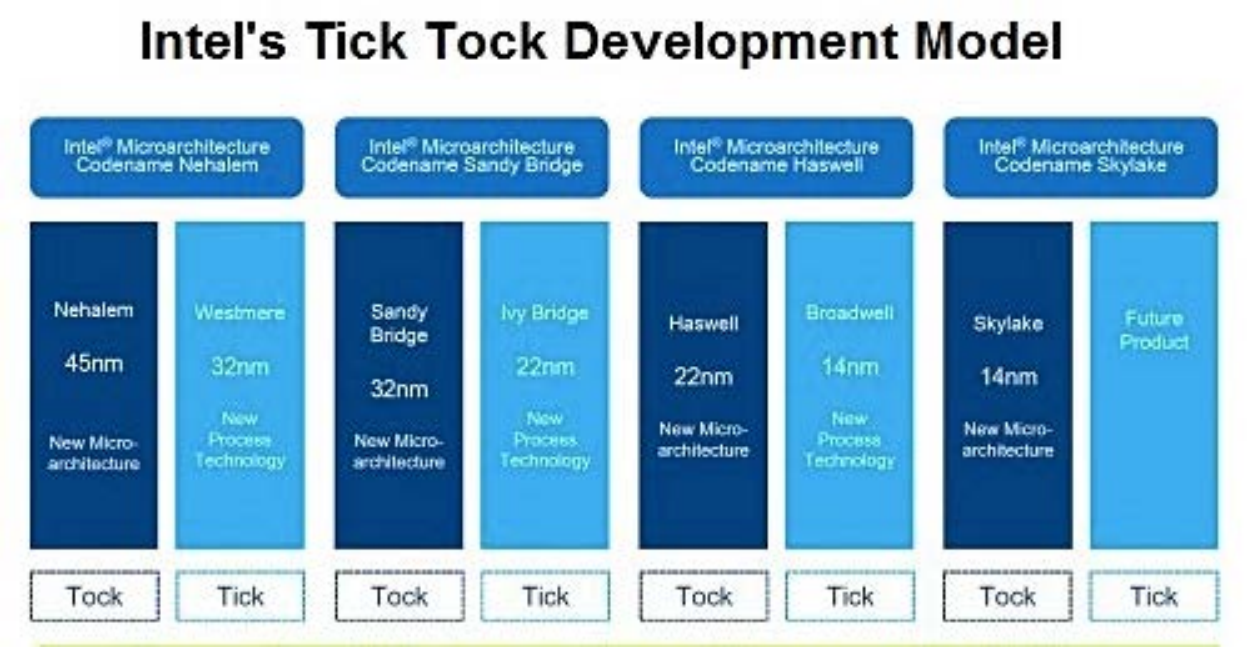
plumbing with very wide pipes and beefing up the pump in order to take full advantage of all this new capacity," Nehalem's design allows the processor to "get much closer to reaching its full potential."[49] Intel also enlarged the "out-of-order" window (e.g., where instructions are executed in dataflow order) by 33% and increased the size of the load, store, and reorder buffers in order to make room for more instructions form predicted branches.

145. Intel also attempted to "deliver a per core performance increase" in Nehalem-based processors. To that end, Intel added a Level 3 or L3 cache that was shared between all of the processors' cores. In prior iterations of Intel's architecture, customers had "to choose between high-performance when all cores [were] active or high performance when only some cores [were] being used." "Having such a shared cache allow[ed] the entire cache to be used by any subset of the cores, in line with [Intel's] goal of not penalizing applications that cannot take advantage of all cores."

146. In addition to addressing per-core performance, Intel designed Nehalem to address the Company's shortcomings in the server space. For instance, Intel re-introduced "hyper-threading" technology in processors. A form of simultaneous multithreading technology, Intel's Hyper-Threading Technology (or HT) allows a CPU to duplicate certain of its resources virtually in order to increase the number of independent instructions in its pipeline. In the server space, HT allows a number of virtual machines to operate seamlessly (and separately) on the same physical server. Accordingly, Intel designed the Nehalem architecture to "further increase the utilization of the [architecture] design" and "to improve the throughput of the core for multi-threaded software environments."

[49] Jon Stokes, *What you need to know about Intel's Nehalem CPU*, *ArsTechnica* (Apr. 9, 2008), https://arstechnica.com/gadgets/2008/04/what-you-need-to-know-about-nehalem/2/.

147. Following the major advances of Core and the Nehalem architectures, Intel continued releasing either a Tick or Tock every 12-18 months until 2016 as follows:



148. With each Tock, Intel sought to enhance its Dynamic Execution (OoOE, speculative execution, and branch prediction) and cache subsystem in pursuit of increased performance of each successive processor. With each Tick, Intel implemented a new manufacturing process known as a process or die shrink. During a process shrink (e.g., moving from 45 nm to 32 nm), the CPU, and in particular, its transistors, are scaled down to fit on a smaller piece of silicon.

149. A process shrink can make a CPU both more powerful and efficient. Smaller transistors mean that more transistors can be packed onto the die, increasing the available power. Less space between the transistors means that information can flow more efficiently, increasing the performance. At the same time, however, the higher number and concentration of transistors also generates more heat. As a result, when it optimized its "Tick" microarchitecture for a new manufacturing process, Intel relied upon shared resources (e.g., shared L3 caches) in an attempt to

balance power, efficiency, and thermal output in its processors, including, in particular, its multi-core processors.

150. In 2016, Intel retired "Tick/Tock" in favor of a new product cycle known as Process-Architecture-Optimization. Under the new product cycle, Sky Lake (formerly a Tock) is now an "Architecture" improvement, with the follow-on microarchitectures, Kaby Lake (2017) and Coffee Lake (2018), considered "Optimizations" of Sky Lake.

9. Intel's Claimed Focus on Security with Core Tick/Tocks

151. Intel understood and appreciated that "protecting the confidentiality of secret or sensitive information is a major concern for users of computer systems."[50]

152. Computer processors are supposed to carry out program instructions in a way that is secure – preventing access to confidential information as they run through the system. Data security is supposed to protect against access to and misuse of personal information, customer's information, business intel and much more.

153. Plaintiffs and absent Class members expected Intel to take adequate security measures and relied on Intel processors to protect and safeguard sensitive and confidential information. Indeed, Enterprise Entities entrusted with sensitive third-party data have legal obligations and duties to protect that data from unauthorized access. Enterprise Entities such as those named as Plaintiffs herein have been and continue to be required to engage in costly mitigation techniques to secure their IT infrastructures because of their statutory and non-statutory duties.

[50] Z. Wang & R. Lee, *New Cache Designs for Thwarting Software Cache-based side channel attacks*, ISCA (2007) at p.1, https://dl.acm.org/doi/pdf/10.1145/1250662.1250723.

154. In particular, healthcare-oriented Enterprise Entities are subject to obligations under the Health Insurance Portability and Accountability Act ("HIPAA"), the American Recovery and Reinvestment Act ("ARRA"), and attendant regulations and other bodies of law. HIPAA establishes a national standard that requires health care providers and their business associates to develop and follow procedures ensuring the confidentiality and security of protected health information ("PHI"), including electronic PHI ("ePHI"), when it is transferred, received, handled, or shared. Healthcare providers are subject to fines of up to $1.5 million by the Office of Civil Rights ("OCR") of the United States Department of Health and Human Services ("HHS") for violations of HIPAA. ARRA requires healthcare providers to make "meaningful use" of electronic health records to engage patients and family and to maintain privacy and security of patient health information.

155. Enterprise Entities also have various other statutory and non-statutory legal obligations and duties to protect and safeguard third party data and information. For example, the Gramm-Leach-Bliley Act ("GLB Act") requires financial institutions – including companies that offer consumers financial products or services (like loans, financial or investment advice, or insurance) – to protect a consumer's nonpublic personal information ("NPI"). Among other things, the GLB Act requires that financial institutions ensure the security and confidentiality of customer's NPI, protect against any anticipated threats or hazards to the security or integrity of customer's NPI, and protect against unauthorized access to or use of customer NPI that could result in substantial harm or inconvenience to any customer.

156. The Enterprise Plaintiffs routinely use Intel CPUs in their servers, PCs, and other devices that are deployed as part of their IT infrastructure to generate, analyze, and store electronic health records ("EHR"), PHI, ePHI and other confidential or protected information. Healthcare

providers also utilize medical devices manufactured by third parties that include Intel CPUs and that gather, analyze, store, and disseminate EHR, PHI, and ePHI. Many healthcare providers also contract with third party cloud-based entities that maintain servers with Intel CPUs that store and disseminate patients' EHR, PHI, ePHI, and other confidential or protected information.

157. Intel clearly understood the importance of security to entities that are subject to HIPAA and other patient privacy laws. Intel's website, for instance, states: "Protection of personal health information is a critical priority. Intel®-based technologies can support the need for compliance with local regulation of health care information such as the HIPAA privacy and security rule." That same web page warned that "[t]he financial impact from security breaches in the United States averaged more than USD 5.2 million per event in 2011."

158. Moreover, beginning with Westmere, the "Tick" following Nehalem, and continuing with each successive Tick/Tock, Intel touted the security of its processors through its vPro offering, often with the tagline, "Secure to the Core."

159. Launched in 2007, vPro included Intel's Active Management Technology ("AMT") and a suite of security technologies for commercial uses of Intel processors including, among others, Intel Trusted Execution Technology ("TXT") and Intel Data Protection Technology (e.g., Intel Advanced Encryption Standards—New Instructions ("AES-NI")). In particular, in *Service Security and Compliance in the Cloud*, Intel Technical Journal, Volume 16, Issue 4, 2012 ("ITJ"), Intel recognized that "[s]ecurity is a key barrier to the broader adoption of cloud computing" (*id*. at 35), and that a fundamental security challenge facing cloud computing is the ability of an unauthorized

user to launch a side-channel exploit to extract information from VMs running on the same system.[51] Intel described TXT as embedded hardware technology in its vPro chips to secure against such risks.

160. TXT is a "hardware-based" technology intended "to protect sensitive information from software-based attacks." To that end, TXT purportedly provided "[h]ardware-assisted methods that remove residual data at an improper [measured launch environment] shutdown, protecting data from memory-snooping software and reset attacks."[52] According to Intel, TXT "addresse[d] the increasing and evolving security threats across physical and virtual infrastructures" and was one of the "building blocks" through which Intel was "setting an industry benchmark for secure processing in data centers."[53]

161. Intel also intended TXT to allow for "[p]rotected execution," whereby an application can "run in [an] isolated environment so that no unauthorized software on the platform can observe or tamper with the operational information."[54] Based on these features, Intel described TXT as a key ingredient for building trusted platforms that allow IT administrators the ability to control virtualized or cloud-based machines able to withstand attacks, including (according to Intel) firmware, rootkit, and side-channel exploits.

---

[51] In connection with its statements, Intel cited to "Ristenpart, T., Tromer, E., et al., *Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds*" CCS'09, Chicago, Illinois, in which the authors warn of the risks of side channel attacks in a VM environment. The authors further noted that these side channel attacks exploit time-shared caches "which appear to be particularly conducive to attacks." *Id.*, ¶ 8.5.

[52] Intel Trusted Execution Technology White Paper, https://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/trusted-execution-technology-security-paper.html.

[53] *Id.*

[54] *Service Security and Compliance in the Cloud*, Intel Technology Journal, Vol. 16, Issue 4 (2012), https://www.intel.com/content/dam/www/public/us/en/documents/research/2012-vol16-iss-2-intel-technology-journal.pdf.

162. AES-NI refers to new instructions that Intel developed to provide "hardware support" for the Advanced Encryption Standard. Adopted by the U.S. Government in 2001, AES relies on cryptography to ensure the confidentiality of communications through an insecure or public/shared channel. Cryptographic functions, though, are traditionally seen as too complex and "computationally costly" to execute efficiently. As Intel explained in a 2010 white paper, "[i]t is expected that when encryption is turned on, performance will degrade."[55] Intel touted AES-NI's ability "to protect data" stored on hardware resources (e.g., processors) shared by several virtual machines in a data center from unauthorized access, use, or alteration through encryption, while removing "the main objection to using encryption to protect data: the performance penalty." In particular, Intel asserted that AES-NI "help[ed] prevent software side-channel attacks."[56]

163. In launching "Haswell" in 2014, the fourth generation of the Core microarchitecture, Intel touted vPro's ability to "protect the OS kernel" from incursions. Intel maintained that its CPUs contained "intelligent security [that] senses when threats are near…. [and] automatically guard[s] your company's data from viruses and malicious attacks with the hardware-assisted technology[.]"

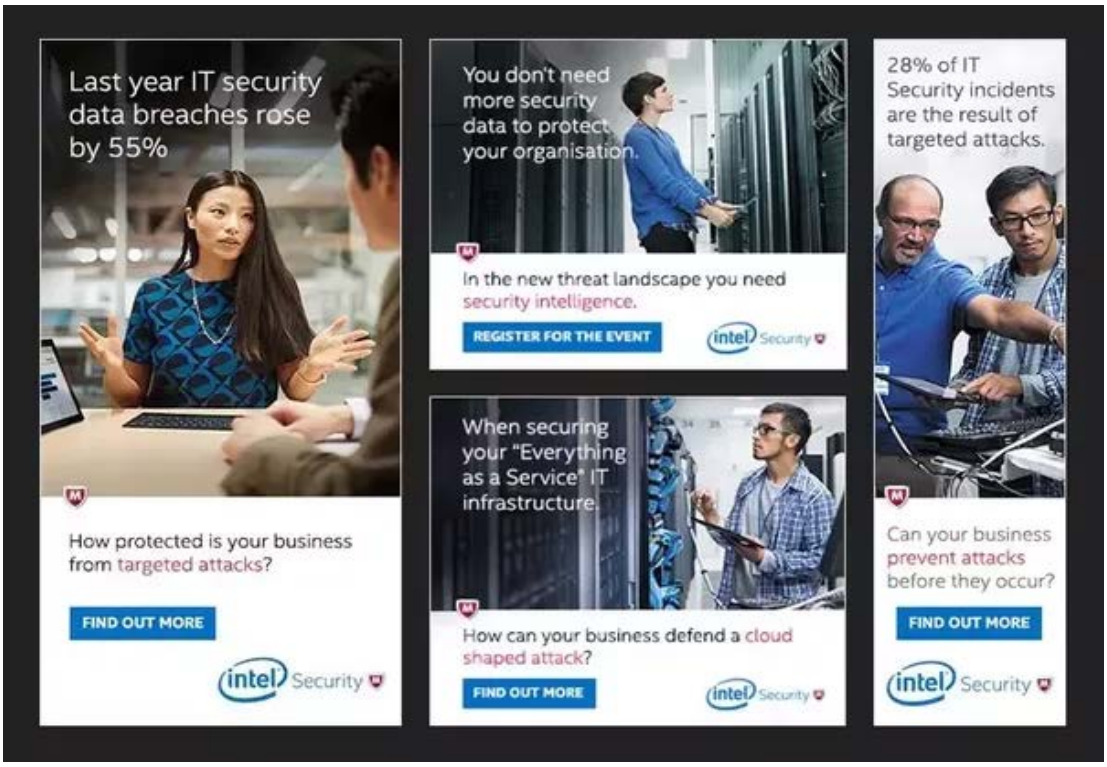
164. What Intel failed to disclose, however, was that the privileged information typically stored within the OS kernel (or other information sufficient to identify the privileged information) was not secure and could be leaked through side-channel exploits on the unsecured caches within Intel's processors.

---

[55] Leslie Xu, *Securing the Enterprise with Intel AES-NI*, Intel White Paper (Sept. 2010) at p. 9, https://www.intel.com/content/dam/doc/white-paper/enterprise-security-aes-ni-white-paper.pdf

[56] Leslie Xu, "Securing the Enterprise with Intel AES-NI" Intel White Paper (Sept. 2010) at p. 5, https://www.intel.com/content/dam/doc/white-paper/enterprise-security-aes-ni-white-paper.pdf.

165. Intel represented to consumers that its CPUs were "secure to the core." It fully appreciated and recognized that many information security standards and regulations require "the protection of sensitive data" and asserted that Intel's processors "stand out" by "extending protection outside the operating system and into the hardware layer."[57] For example, Intel touted its hardware-based security to protect against malicious attacks:



166. According to Intel, "[i]f you own a business, you're at risk…. Virus protection and other software solutions—though useful and necessary—only get you so far …. So what can you do to stay safe? Don't rely on software alone. You need your hardware to do the heavy lifting."[58]

[57] Intel Product Brief, *Building A Secure Digital Learning Environment*, Intel https://www.intel.com/content/dam/www/public/us/en/documents/brochures/authenticate-product-brief-english.pdf (last visited May 5, 2020).

[58] *Could Your Old PCs Be Putting Your Business at Risk?*, Intel IT Peer Network (Feb. 16, 2016), https://itpeernetwork.intel.com/could-your-old-pcs-be-putting-your-business-at-risk/#gs.60gfpu.

Intel assured consumers that "Intel Core processors ha[d] hardware-enhanced security features that allow hardware and software to work together, protecting your business from malware and *securing the important, private data and content* you create and share:[59]

[59] *Id.* (emphasis added).


intel
Old PCs put your business at risk
Protect against hackers by upgrading to new desktops featuring Intel's hardware-enhanced security and supporting software
The risk
Software-only security solutions from even a few years ago can't keep up with today's cybercriminals and are not sufficient to protect your devices and vital business data. Without hardware-enhanced security solutions, your business is at risk.
The opportunity
The newest generations of Intel® processors deliver layers of hardware-enhanced security features to ensure that hardware and software work together to protect your business from malware and secure all the important, private data and content you create and share.
The next step
Don't wait to be attacked. Secure your business now by replacing computers purchased before mid-2013 with new desktops that include Intel hardware-enhanced security features.
With hackers working around the clock to identify the next potential victim, it's more important than ever for you to prioritize security. And if your business is using PCs even just a few years old, the chances of a successful attack are even greater: Virus protection and other software security solutions cannot sufficiently reduce the risk.
What you're up against: Three tools of the modern hacker
Here are three of the most common—and dangerous—ways that hackers can attack your desktops, infect them with malware, and harm your business:
Intel® IPT
Intel® OS Guard
Intel® AES-NI
Windows® 8 Bootup Security
Intel® SSD Pro
Advanced Persistent Threat
These insidious, human-directed "campaigns" take control of a specific system or network and can remain undetected for a long period of time.
Social Engineering
Hackers manipulate people to divulge sensitive data, using tools that lure users to sites or by sending "phishing emails" that trick unsuspecting users into giving up their login credentials. Even the most sophisticated people can sometimes be persuaded—it can happen to anyone.
Kernel-Mode Rootkit
Often used to deliver "Trojan Horses" and other malware code, these attacks live and operate below the operating system, making them especially hard to detect without some kind of hardware assistance.
What you can do to make your business more secure
Innovative hardware enhancements, built into Intel®-powered desktops since mid-2013, "harden" key information and commands normally executed in software, giving your business maximum protection. Get new business desktops with Intel® Identity Protection Technology (Intel® IPT), Intel® OS Guard, Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI), Intel® Solid-State Drive Pro (Intel® SSD Pro), and bootup security for Microsoft Windows® 8 and increase your organization's security today.

167. With the launch of "Skylake" in 2015, the sixth generation of the Core microarchitecture, Intel touted the CPUs' "cutting-edge security,"[60] claiming "[t]he Skylake architecture has been designed to enable better security"[61] not just for enterprise consumers through the vPro platform[62] but all consumers "at home." Intel asserted consumers were "safe and secure at home" "knowing all of [their] pictures, videos, and personal files [were] securely stores at home." The "6th gen Intel Core processors with hardware-based security features help keep your system and data free from malware, hacking, viruses, and prying eyes."[63]

168. Similarly, prior to January 2018, Intel recognized that cyber-attacks were "moving down the computing stack, traversing from software to hardware, threatening devices in homes, cars, businesses, networks and cloud," making it such that "[t]he legacy model of software protecting software can't keep up with advancing threats against digital security, safety and privacy." To address this known threat, Intel designed "hardware-enabled security capabilities"

---

[60] *Top Reasons to Modernize Your Agency with the 6th Gen Intel Core vPro Processor Family*, Intel, https://www.intel.com/content/dam/www/public/us/en/documents/sales-briefs/modernize-with-6th-gen-core-vpro-brief.pdf (last visited May 5, 2020).

[61] *Intel Sets New Standard for Computing with 6th Gen Intel Core Processor Family and Intel Xeon Processors for Mobile Workstations – Intel's Best Processors Ever*, Intel News Fact Sheet, http://download.intel.com/newsroom/kits/core/6thgen/pdfs/6th_Gen_Intel_Core-Intel_Xeon_Factsheet.pdf (last visited May 5, 2020).

[62] Intel News Fact Sheet, *Intel Sets New Standard for Computing with 6th Gen Intel Core Processor Family and Intel Xeon Processors for Mobile Workstations – Intel's Best Processors Ever*, Intel http://download.intel.com/newsroom/kits/core/6thgen/pdfs/6th_Gen_Intel_Core-Intel_Xeon_Factsheet.pdf (last visited May 15, 2020),

[63] *Safe and Sound at Home with Desktop PCs*, Intel https://www.intel.com/content/www/us/en/desktops/desktop-storylines-security-infographic.html (last visited Aug. 24, 2018) *Note: since the filing of Plaintiffs' Consolidated Class Action Allegation Complaint, Intel has removed this advertisement infographic from its website. Archived versions are available at web.archive.org,* http://web.archive.org/web/20170423053311/http://www.intel.com/content/www/us/en/desktops/desktop-storylines-security-infographic.html.

directly into its processor, thereby allowing the CPU to protect the computing ecosystem "against evolving and modern threats."[64] Ultimately, although Intel touted its "leading edge security," its decision to sacrifice security in its implementation of speculative execution led Intel's CPUs to be uniquely exposed to several major categories of exploits—Meltdown, Foreshadow, Fallout, RIDL, ZombieLoad, SwapGS, LazyFP, Vector Register Sampling, CacheOut, L1D Snoop Sampling, and likely numerous yet-to-be-disclosed exploits.

B. Intel's Processors Are Defective

1. Security Vulnerabilities Created by Intel's Use of Speculative Execution and an Unsecured Cache Subsystem Lead to Confidentiality Security Breaches

169. Ensuring the "confidentiality" of secret, sensitive, or private information by preventing its disclosure to an unauthorized entity is one of the most basic security properties, and an obligation Intel and its competitors in the industry acknowledged and accepted when designing new CPUs to release in the market.

170. Hardware plays a central role in security. "Fundamental to almost any security question is the idea of a secret. Whether a secret is cryptographic key, or merely a hidden certificate, a secure processor must be able to generate, protect, and share that secret with the outside world."[65]

[64] Hardware – Enabled Security Powered by Intel Technology, *Strengthening Security Protection*, WaybackMachine (Apr. 7, 2017), https://web.archive.org/web/20170407073442/https://www.intel.com/content/www/us/en/security/hardware/hardware-security-overview.html (last visited May 5, 2020).

[65] G. E. Suh, et al., *Design & Implementation of the AEGIS Single-Chip Secure Processor Using Physical Random Functions* (2005), p. 1, http://csg.csail.mit.edu/pubs/memos/Memo-483/Memo-483.pdf.

171. One way to protect the confidentiality of sensitive information is by controlling access to the information such that only authorized users can read or modify it.[66] Since 1985, Intel microarchitecture designs have relied upon protected mode and virtual memory to ensure that sensitive information is protected from unauthorized access.

172. A "security attack" or exploit is a specific action that can cause a "security breach" or an event that violates a basic security property. It is characterized by a detailed description of the vulnerability exploited, the path of attack, and the subject of the exploit. Critically, exploits that breach confidentiality are hard to recover from because once the information is disclosed, it is already too late.[67] A "security vulnerability" is a weakness in the system that can be exploited in a security attack.[68]

173. Unbeknown to Plaintiffs and members of the Class, Intel intentionally sacrificed security, defied well-settled architecture design principles, and permitted unauthorized program instructions to access protected memory—all to achieve increased speed. Specifically, and as explained herein, Intel's implementation of Dynamic Execution created security vulnerabilities within its CPUs, rendering them defective. For example, Intel undermined the security of its processors by implementing OoOE and speculative execution in a way that (i) created windows of time during which an unauthorized user could have the processor make unnecessary or unauthorized memory accesses to copies of sensitive or privileged information (i.e., Unauthorized Access) and (ii) allowed that information (or critical data about the location or contours of that information) to

[66] Ruby B. Lee, *Security Basics for Computer Architects* (2013).

[67] *Id.*

[68] *Id.*

remain in the CPUs' caches after the mistaken or unauthorized access (e.g., an exception) was discovered (i.e., Incomplete Undo).

174. Intel likewise undermined the security of its processors by implementing a shared cache design that did not (i) include any mechanism to ensure that sensitive or privileged information (or data concerning that information) was flushed once the processor determined it had unnecessarily or improperly accessed memory, or (ii) provide any protection against side channel exploits that use the cache to siphon out data that remains in the cache after a processor completes its tasks.

175. As explained below, Intel knew that its processors, and in particular, the CPUs' cache subsystems, were vulnerable to side-channel exploits, and that side-channel exploits could be used to "leak" confidential information that was exposed as a result of Intel's implementation of OoOE and speculative execution in its CPUs.

2. Intel Knew That Its Architecture Was Susceptible to Side-Channel Exploits

176. Leaking information through covert or side-channels is one type of security exploit that can lead to a confidentiality security breach. In a side-channel exploit, an unauthorized actor exploits a security vulnerability to access or monitor information about the implementation of a computer system for the purpose of learning about or accessing otherwise privileged information. In this way, private information is deduced from observing the side-effects of operations. Such exploits need not depend on software bugs. Instead, as described here, they can exploit hardware vulnerabilities.

177. In a "timing" side-channel exploit, an unauthorized actor exploits a security vulnerability with the express purpose of obtaining information about how long it takes the computer

to complete a task, in order to infer something about otherwise privileged information. If someone can determine how long it takes a CPU to fetch instructions or data it needs to complete its operations, he can infer where the information is located within the system, and, ultimately, the substance of the information.

178. In particular, it takes less time to access data that resides in a processor's cache subsystem than data that must be retrieved from main memory. By measuring the amount of time it takes for a processor to fetch instructions or data, an unauthorized user can learn whether the requested information is in the cache or in main memory. If certain data is stored within the cache subsystem or "cached," an unauthorized user then knows that it has been accessed recently. Once an unauthorized user has access to these measurable differences in the amount of time it takes to access different kinds of information, he can discern the underlying information.

179. Consider the following analogy. An individual (e.g., the unauthorized user) goes to a library (e.g., the computer) to read a book (e.g., data) from a special collection the individual does not have permission to access (e.g., kernel memory). The individual asks the librarian to retrieve "Special Book #1 and the Sue Grafton novel that corresponds to the first letter of page 1 of Special Book #1," (e.g., a program instruction). The librarian retrieves (e.g., fetches) Special Book #1 from the special collection and determines (e.g., decodes) that the first letter on page 1 of that book is "C," requiring the librarian to also retrieve "C is for Corpse," by Sue Grafton. The librarian returns to the front desk with Special Book #1 and "C is for Corpse" by Sue Grafton. Before the librarian shows the individual the requested books, she checks his library card. If the librarian determines that the individual does not have permission to access books in the special collection, she will put the books on a cart to be re-shelved (e.g., the cache) without showing them to the individual.

180. Knowing that the Sue Grafton book with the title corresponding to the first letter on the first page of Special Book #1—the book the individual wants to read but does not have permission to access—is now on the cart, the individual begins methodically requesting Sue Grafton books, starting with "A is for Alibi." If the librarian responds to this request with "please wait while I go and retrieve that book," the individual knows that book is not on the re-shelving cart and the first letter on the first page of Special Book #1 is not A.

181. When the individual requests "C is for Corpse," however, the fact that the librarian is able to quickly retrieve it from the re-shelving cart reveals to the individual that the first letter on page 1 of the Special Book #1 is "C." If it takes nanoseconds to complete these tasks (as it would within a CPU), the individual could determine fairly quickly the contents of Special Book #1 without ever actually seeing the book itself. In the same way, a timing side-channel exploit on a CPU cache allows an unauthorized actor to gather enough data about where sensitive or privileged information is located within the computer to deduce the precise contours of that sensitive or privileged information.

182. Although unknown to the consuming public, the susceptibility of Intel's cache design to side-channel exploits was described by researchers and academics in highly technical research papers concerning early iterations of its processors. In fact, discussions of the fundamental problems that underlie the vulnerabilities appear in computer science literature from the early- to mid-1990s. For example, Olin Sibert *et al.*, *The Intel 80x86 Processor Architecture: Pitfalls for Secure Systems* (1995), identified exploitable weaknesses in Intel's microarchitecture and explained that caches may be used as covert timing channels to leak sensitive information. *Id.*, § 3.10 (citing Wray, *An Analysis of Covert Timing Channels* (1991)). The authors of the article emphasized that the imbalance in scrutiny of hardware security had already become "untenable" and "increasingly difficult to justify."

Id., §§ 1, 2.[69] Intel's design response and associated micro-architectural changes to address these and other expressed security concerns have been largely confidential.

183. In a 2010 white paper entitled, *Securing the Enterprise with Intel AES-NI* (Sept. 2010), Intel described an on-going problem with AES cryptographic keys, noting that "in multiple processing environments . . . a piece of malicious code running on the platform could seed the cache, run cryptographic operations, then time specially crafted memory accesses to identify changes in the cache. From these changes, the unauthorized user could determine portions of the cryptographic key value"[70] which can then be used to defeat AES encryption. To solve this problem, Intel launched AES-NI, *see supra*, which protected AES cryptographic keys from side-channel exploits by ensuring that this information was never stored in the CPU's caches. Despite knowing that the root cause of the side-channel exploit against AES was an unauthorized user's ability to "seed the cache" and "identify changes in the cache," Intel did not secure the cache subsystem from side-channel exploits. Though Intel implemented AES-NI to help avert cache timing side-channel exploits against AES by eliminating the use of cache for AES calculations, it did nothing to address Intel's fundamental defective design choices.

184. The vulnerability created by Intel's decision to leave the cache subsystem unsecured is exacerbated when the cache is shared among the CPU's threads and cores. For over a decade,

---

[69] *See also* Paul C. Kocher, *Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems*. Advances in Cryptology—CRYPTO, Vol. 1109 Lecture Notes in Computer Science, 104-113 (1996) (a seminal work on timing attacks, which noted the potential to exploit timing measurements from vulnerable systems to find entire secret keys, and specifically referenced RAM cache hits as a source of such exploitable timing differentials), https://www.paulkocher.com/doc/TimingAttacks.pdf.

[70] Leslie Xu, *Securing the Enterprise with Intel AES-NI*, Intel White Paper (Sept. 2010), at p. 5-6, https://www.intel.com/content/dam/doc/white-paper/enterprise-security-aes-ni-white-paper.pdf.

Intel knew, or reasonably should have known, that unauthorized users could exploit a CPU resource (such as a cache or buffer) that is shared by two processes running simultaneously on the CPU. In effect, one process may "spy" on the other by examining changes made to that shared resource by the other process.

185. Computer security researcher Colin Percival demonstrated one exploit of this kind in late 2004. Percival showed that on Intel CPUs with a "Hyper-Threading" design, where multiple threads (i.e., processes) are scheduled to run simultaneously on the same processor, the use of shared memory caches allowed an unauthorized process to make deductions about the other program's behavior and steal information, in this case, cryptographic keys. Percival described having caches shared between threads as a vastly dangerous avenue of attack. He notified Intel of this problem in early 2005, prior to presenting his paper describing the exploit, *Cache Missing for Fun and Profit* (2005).[71] At approximately the same time, another group of researchers published a work that similarly showed exploitation of the shared cache through two techniques.[72]

186. The exploit Percival detailed is one variation of the same basic theme—an unauthorized actor exploiting the changes a process causes to the micro-architectural state of a CPU

[71] *See* Colin Percival Daemonic Dispatches Blog, *Some thoughts on Spectre and Meltdown*, Daemonlogy.net, http://www.daemonology.net/blog/2018-01-17-some-thoughts-on-spectre-and-meltdown.html (last visited May 5, 2020); *see also* Colin Percival, *Hyper-Threading Considered Harmful*, Daemonlogy.net, http://www.daemonology.net/hyperthreading-considered-harmful/ (last visited May 5, 2020).

[72] In Osvik, *et al.*, *Cache Attacks and Countermeasures: the Case of AES* (2005), the group explained that unauthorized users could mount a powerful attack by determining which cache sets had been accessed by a victim program. First, in an attack known as Evict + Time, and unauthorized user measures how execution time is influenced by evicting a chosen cache set to see whether a particular cache set was used by a victim. Second, in a Prime + Probe attack, the unauthorized user can get better accuracy by measuring cache access times directly rather than indirectly through execution time. https://www.cs.tau.ac.il/~tromer/papers/cache.pdf.

(in particular, a shared memory cache) in order to acquire another's information. In fact, any time a resource is shared, there is a possibility information can leak. For example, if one CPU core asks whether certain data is present in the L3 cache, the answer, a binary yes or no, provides some useful information about the current work the CPU is engaged in. If an unauthorized actor can access that information and analyze it, it could lead the actor directly to secret or privileged information thought to be protected in other parts of the computer.

187. In a 2006 paper, *Covert and Side Channels Due to Processor Architecture*, Dr. Ruby Lee and Zhenghong Wang, examining a different Intel processor family, presciently highlighted a new "speculation-based covert channel," arising from the fact that when Intel allows a load instruction to execute speculatively in the IA-64, although a bit is set in the register if the speculative load instruction would cause an exception, the exception is not handled right away. Instead, "[c]ontrol speculation allows deferral of the exception," including exceptions such as access violations, thereby opening the door for unauthorized users to leak information via a side-channel exploit. *Id.*, § 3.4.

188. Dr. Lee has emphasized that software-based solutions still left the "crown jewels of primary key material" susceptible to attack and that "[a]ll current processors with caches are vulnerable—from embedded devices to cloud servers."[73] In a paper published in 2007, in which Lee and Wang discuss thwarting side-channel exploits at the root, the authors cautioned that "[c]ache-based side channel attacks can be very dangerous" and "very effective."[74]

---

[73] R. Lee, *University Research in Hardware Security*, Hotchips.org (Aug. 10, 2014), https://www.hotchips.org/wp-content/uploads/hc_archives/hc26/HC26-10-tutorial-epub/HC26.10-tutorial1-HW-Security-epub/HC26.10.155-6_Lee_UniversityResearch_go.pdf.

[74] Wang *et al.*, *New cache Designs for Thwarting Software Cache-based Side Channel Attacks* § 7 (2007).

189. At approximately the same time that Dr. Lee's paper was published, an analogous side-channel exploit that exploited speculative execution and a shared CPU resource called the Branch Target Buffer (or "BTB"), used in branch prediction, was described. *See* Acıiçmez *et al.*, *Predicting Secret Keys via Branch Prediction* (2006). Using the described exploit, an unauthorized actor could determine private cryptographic keys used in the target user's computer.

190. Later, in 2013, Yuval Yoram demonstrated a cache-based side-channel exploit that showed that the unauthorized user and victim process need not share the execution core. *See* Yoram *et al.*, *Flush+Reload: A High Resolution, Low Noise, L3 Cache Side-Channel Attack* (2013). In this cross-core attack, as long as the processes had shared use of the cache, the unauthorized user could identify the target's access to specific memory.[75] The crux of the exploit is a weakness in Intel's X86 architecture; specifically, the lack of permission checks before permitting use of an instruction that allows an unauthorized user to evict specific memory lines from cache. As the researchers observed, "Not restricting the use of the instruction is a security weakness of the Intel implementation of the X86 architecture," which "requires a hardware fix."[76] The authors cautioned that "[g]iven the strength of the attack, . . . the memory saved by sharing pages in a virtualized environment does not justify the breach in the isolation between guests."

[75] This could be accomplished through a "Flush + Reload" technique in which (1) the unauthorized user flushes a memory line from the cache, then (2) waits to give the victim an opportunity to access the memory line, and then (3) the unauthorized user reloads the memory line, which will be quick if the victim did in fact access the line (since it is now back in cache) or will be significantly longer if the victim did not access the line, which then needs to be brought in from main memory. https://eprint.iacr.org/2013/448.pdf.

[76] The authors note that ARM architecture also includes an instruction to evict cache lines but that it can only be used when the processor is in an elevated privilege mode. https://eprint.iacr.org/2013/448.pdf.

191. That same year, researchers described a side-channel exploit for deducing information about privileged address space layout which can be used to defeat a common memory management security technique called kernel address-space-layout randomization ("KASLR").[77] Those exploits against Intel x86-based processors (specifically, Intel i7-870, Intel i7-950, and Intel i7-2600) are enabled because "hardware (such as caches and physical memory) are *shared* between privileged and non-privileged code" and "the nature of the cache facilities still enables an unauthorized user to indirectly measure certain side-effects." Hund at 195 (emphasis in original).

192. By 2015, Intel knew, or reasonably should have known, that an unauthorized user could mount a cache side-channel without the need to install code on a victim's machine. In Oren, *et al.*, *The Spy in the Sandbox: Practical cache Attacks in Javascript and their Implication* (2015), the authors described a cache side-channel exploit that ran entirely in a web browser. Thus, "the victim needs only to browse to an untrusted webpage that contains attacker-controlled content" to facilitate an attack. *Id*. at Abstract.[78]

193. Thus, research papers describe cache side-channel exploits that exploit Intel's decision to lessen the security of its CPUs—while seeking additional performance to further marketing claims—and thus gain access to kernel memory and other privileged information.

194. The types of highly technical/academic research papers that reported on side-channel exploits, however, are not commonly viewed by the general public buying Intel's CPUs and

[77] *See* Hund *et al.*, *Practical Timing Side Channel Attacks Against Kernel Space ASLR* (2013) ("Hund"), https://www.ieee-security.org/TC/SP2013/papers/4977a191.pdf.

[78] Using their Javascript-based cache side channel attack, the authors were able to map more that 50% of a victim's cache in as little as one minute and gain access to the victim's mouse movements and network activity (i.e., websites visited).

products containing them, given the sophisticated and specialized nature of the papers. Rather, these types of research papers are often aimed at industry insiders, such as Intel, and academics.

195. Moreover, while Intel hid from Plaintiffs and members of the Class that these vulnerabilities pose a severe security threat, in various patent filings Intel acknowledged the security risks caused by cache side-channel timing exploits. Intel was aware that its hardware design could be used to leak privileged information, and even claimed knowledge and awareness of means to modify its chip designs to prevent such exploits. *See Mitigating Branch Prediction and Other Timing Based Side Channel Attacks*, U.S. Patent No. 8,869,294 B2 (filed Dec. 5, 2007) (the "'294 patent") ("New mitigations to side channel attacks are needed to deter attempts to subvert the security of a computer system.") col. 1, lines 45-46; *Protecting Private Data From Cache Attacks*, U.S. Patent No. 8,516,201 (Dec. 5, 2007) (the "'201 patent") ("Cache-based side channel attacks have recently become a concern for applications that perform cryptographic operations . . . . Side channel attacks are also possible when two applications share the same cache.") col. 1, line 63-col. 2, line 5; *Protected Cache Architecture and Secure Programming Paradigm to Protect Applications*, U.S. Patent No. 8,341,356 B2 (filed May 3, 2011)[79] (the "'356 patent") (proposed invention "to prevent a so-called side channel attack in which an attacker program and a victim program . . . both use the same physical cache.") col. 2, lines 5-8; *Obscuring Memory Access Patterns in Conjunction with Deadlock Detection or Avoidance*, U.S. Patent No. 8,407,425 B2 (filed Dec. 28, 2007) (the "'425 Patent") ("side-channel attacks exploit aspects of multi-threading environments where two concurrent threads share computing resources" and "[o]ther exploits that use this type of information leakage may be readily envisioned") col. 1, lines 18-26.

[79] The provisional application No. 60/873,051 was filed Dec. 5, 2006.

196. As such, Intel's CPUs are materially defective—and Intel knew it. When Intel's processors engaged in speculative execution, the processors rendered information that should have remained secure and inaccessible to unauthorized use, accessible in the processors' unsecured cache subsystem. In so doing, Intel's processors created a vast security vulnerability that could be accessed through a number of different exploits.

197. Incredibly, despite its knowledge of the risk of side channel attack and its flawed processor design, Intel concealed that it had implemented the Unauthorized Access Defect and failed to redesign to make its CPUs safer or revert to the security it had implemented in the P6 architecture but subsequently removed to achieve increased performance. As ordinary consumers, Plaintiffs and members of the Class did not know (and had no way of learning) that Intel had permitted unauthorized access to protected data—which was directly contrary to the message about the security of its hardware security that Intel touted.

3. Intel Knew That Permitting Unprotected Memory Access During Speculative Execution Could Be Exploited

198. Intel's implementation of speculative execution in its processors created a window of time during which an unauthorized user could make unnecessary or unauthorized requests to access memory for information. As alleged and explained above, when a processor engages in speculative execution it fetches information it needs to execute instructions out of program order, allowing the CPU to avoid performance penalties when it encounters data dependent or conditional instructions. These requests could be legitimate, e.g., the application requests access to information that is not itself privileged, but unnecessary (i.e., the information ultimately will not be utilized by the processor). These requests also could be illegitimate—e.g., the application requesting access to privileged information is not authorized to do so. Irrespective of the necessity or legitimacy of the

request to access memory, the information fetched from memory was stored in the CPU's caches and buffers (a type of cache that assists the processor in transporting information from one process to another) until it was needed.

199. Intel designed its processors to avoid taking any action to address unauthorized (e.g., exceptions) or unnecessary (e.g., mistakes) memory requests until such time as the processor was ready to retire the instructions in program order. This allowed the CPU to defer action on any mistakes or exceptions encountered during out-of-order or speculative execution until the end of the process to enhance the processor's performance. Intel's decision to defer these actions, however, allowed, without permission, sensitive or privileged information (or data about that information) to be transferred to and maintained in the CPU's caches or buffers.

200. Intel's implementation of out-of-order or speculative execution created a window that remained open until the instruction necessitating out-of-order or speculative execution in the first instance was complete—e.g., in the case of a conditional instruction (if X, then Y), when the CPU determines the correct branch direction and target. It was only after the window closed that Intel's processors addressed any mistakes (e.g., a mis-predicted branch where the memory access was legitimate but unnecessary) or exceptions (e.g., an application accessing data with insufficient privileges) that occurred while the CPU was engaged in out-of-order or speculative execution, and then flushed its pipelines of any impact from the related instructions.

201. The information fetched for instructions executed out-of-order or speculatively, however, remained behind in the CPU's caches and buffers. In other words, while its processors should have rolled back any impacts of executing unnecessary or improper instructions on the computer, Intel allowed the raw materials the CPU fetched to execute these instructions to remain in the processors' caches or buffers, and thus vulnerable to unauthorized access.

202. Intel relied on speculative execution to increase the performance of its processors even though it knew that, as Dr. Lee and her co-author, Wang, explicitly warned as early as 2006, the deferral of exceptions "can be exploited to facilitate information leakage."[80] Six years later, Wang again warned of the risks of speculation-based side-channel attacks in his doctoral thesis, *Information Leakage Due to Cache and Processor Architectures* (Nov. 2012), on which Dr. Lee was the advisor, stating, "[w]e wish to emphasize the severity of this channel before real damage is done." *Id*. at 81.

203. Intel likewise knew through at least two other instances that the Company's decision to permit unchecked memory accesses in its processors presented a serious security vulnerability, exploitable by unauthorized users siphoning information out of the processor cache through a side-channel attack—the "Prefetch Side Channel Attack" and the "TSX Side Channel Attack."

204. **Prefetch Side-Channel Attack.** Intel's processors include a function known as "prefetch," with which a software program can direct the CPU to fetch data before it is needed. According to Intel, the prefetch instruction "can hide the latency of data access in performance-critical sections of application code by allowing data to be fetched in advance of actual usage." Because prefetch "merely provides a hint to the hardware," its usage "*generally does not generate exceptions or faults*" in the CPU. As explained in *Prefetch Side-Channel Attacks: Bypassing SMAP and Kernel ASLR* (2016), though, "[p]refetch instructions on Intel CPUs *ignore* privilege levels and access permissions" making it possible for any unauthorized user to use prefetch to access "inaccessible kernel memory" and then execute a cache-based timing side-channel exploit to access

[80] Wang, *et al.*, *Covert and Side Channels due to Processor Architecture* (2006), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.190.1003&rep=rep1&type=pdf.

the data put in the cache by the prefetch function. *Id.* § 3.2. The authors of *Prefetch Side-Channel Attacks* noted that Intel reference manuals from 2014 (and, indeed, by as early as 2012) reflect that the "prefetch" command could be used to access illegal or unprivileged memory space without generating any exceptions.

205. **TSX Side-Channel Attack.** In 2016, researchers revealed a timing side-channel exploit that exploited an Intel hardware feature called Transactional Synchronization Extension (TSX). As researchers explained:

> One surprising behavior of TSX, which is essentially the root cause of this security loophole, is that it aborts a transaction without notifying the underlying kernel even when the transaction fails due to a critical error, such as a page fault or an access violation, which traditionally requires kernel intervention.

Jang *et al.*, *Breaking Kernel Address Space Layout Randomization with Intel TSX* (Oct. 2016) ("Jang") at 380.

206. In other words, with TSX, the processor allowed a thread to perform a sequence of operations inside a transaction and if an exception due to unprivileged access occurs, the OS will not be notified. Instead, the exception will be suppressed, meaning, as stated in Intel's September 2016 manual, transactional execution would abort and it will be as though the exception or fault had never occurred. *See* https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developers-manual.pdf. The authors noted that because TSX suppresses exceptions, such as an access violation that is caused by accessing kernel space from a user process, TSX "exposes a clear, stable timing channel." Jang at 382. Jang went on to describe a side-channel attack exploiting the suppression of exceptions by TSX that can "extract the executable and non-executable bit of every kernel page and defeats KASLR ("Kernel Address Space Layout Randomization"). *Id.* Thus, the TSX side-channel exploit, like the Prefetch Side-Channel

Attack, is another instance in which Intel's suppression of exceptions was exploited by a timing side-channel exploit to gain access to kernel information.

207. Intel knew, or should have known, that just as its suppression of exceptions under Prefetch and TSX could be exploited by a timing side-channel exploit, the decision to defer taking action on memory access violations under speculative execution could also be exploited by side-channel exploits. This is precisely what occurred in Meltdown, Foreshadow, and Spectre.

4. "Meltdown"

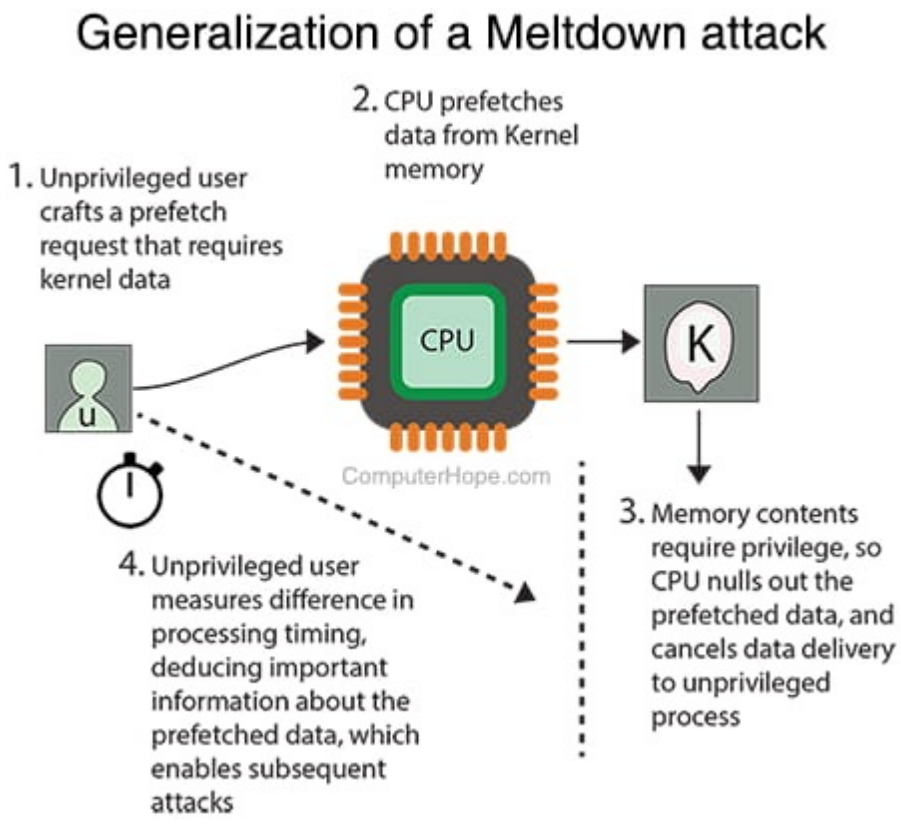
208. In July 2017, researchers identified "Meltdown" or "Rogue data cache load" (CVE-2017-5754), also known as "Variant 3," and informed Intel of this particular type of side-channel exploit. The exploit was nicknamed "Meltdown" by researchers due to its ability to effectively dissolve the informational barrier that protects privileged data, allowing an unauthorized user to read sensitive information like passwords, login keys, and encryption keys.

209. Meltdown takes advantage of both the Unauthorized Access and Incomplete Undo Defects inherent in Intel's CPUs.

210. Specifically, speculative execution fetches data *before* enforcing a privilege check to confirm that the user is authorized to read such data. Intel designed its CPUs to forgo this critical privilege check so that its chips could run faster. If it turns out that the user attempting to access the data possesses the appropriate privilege level, allowing access to the data "speculatively" (*i.e.*, without first checking and enforcing access permissions) saves time. On the other hand, if the user lacks the appropriate privilege level, an error or "exception" occurs and the user should be denied access to the privileged data. Intel's defective CPUs, however, defer enforcement of the exception thereby creating a window of time where an unauthorized actor can gain unauthorized access to

privileged information (or secrets) present in the operating system's "kernel" memory, which is the most protected memory on a computer.

211. By engineering a system that permits access to privileged information/secrets in a manner that allows a user to win a "race condition" between the instruction execution and the delayed enforcement of a privilege check, the unauthorized user gains a window of time to deploy a side-channel exploit to infer the privileged information/secrets from data contained in the cache. This is Meltdown in a nutshell.



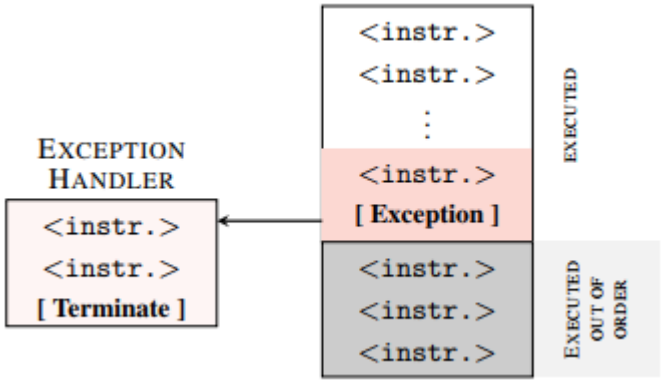
https://www.computerhope.com/jargon/m/meltdown-and-spectre.htm.

212. The first step in a Meltdown exploit is to run instructions that attempt to load the cache with an address that the unauthorized user has rights to and that depends on secret data, which ordinarily triggers an exception:

```
1 ; rcx = kernel address
2 ; rbx = probe array
3 retry:
4 mov al, byte [rcx]
5 shl rax, 0xc
6 jz retry
7 mov rbx, qword [rbx + rax]
```

https://meltdownattack.com/meltdown.pdf.

213. Because of speculative execution, the subsequent instructions to move the inaccessible address are executed speculatively and out of order, before the exception is handled, thereby loading the secret value into the cache without enforcing the privilege check on the user:



https://meltdownattack.com/meltdown.pdf.

214. In order to ensure that all of the necessary instructions to complete the exploit are speculatively executed before the exception is triggered, a Meltdown exploit may exploit "exception handling" or "exception suppression" techniques that prevent the OS from terminating the program as soon as the exception is triggered. Once the exception is handled, the program is terminated, but the secret data remains in the cache and is not flushed.

215. Finally, a Meltdown exploit uses a side-channel exploit, such as "Flush+Reload," to repeatedly probe the contents of the cache by flushing and reloading its contents while monitoring small differences in the time it takes to access the loaded cache block. Through this process, an

unauthorized user can determine where in the cache the privileged memory was stored and deduce the contents of that memory. For example, assuming the secret data is the value "15," the unauthorized user will probe cache blocks 1-15. If the timing differences in flushing and reloading the cache indicate that block 15 is present, the unauthorized user can infer that the secret data is 15.

216. By repeating these steps, an unauthorized user can read not only "kernel" memory, but because all major operating systems also typically map the entire physical memory into the kernel address space, an unauthorized user can also read the entire physical memory of the target machine.[81] The result is that a bad actor can entirely bypass the privilege-mode isolation on a machine to access its most sensitive and confidential information, like secret passwords, without detection.

217. Meltdown is extremely similar to the Prefetch Side-Channel Attack. For instance, both the Meltdown and Prefetch Side-Channel Attack "melt down" the boundary between user space and kernel space and exploit Intel's failure to enforce privilege checks and access permissions prior to granting access to kernel memory. Additionally, the team that discovered Meltdown used the exception suppression "feature" of TSX to carry out their Meltdown exploit. *See* Lipp *et al.*, *Meltdown: Reading Kernel Memory from User Space*, at p. 6.

[81] Kernel memory addresses are mapped in the user process's virtual address space and corresponding page table (along with the user's own virtual memory addresses). This is done so that when a switch into kernel mode is required, e.g., because of either a system call (i.e., asking OS to do something) or an interrupt happens, the switch to kernel mode can be done quickly since the kernel addresses are already mapped in the page table for the user's address space. Kernel memory address ranges are marked as non-accessible so that the user program itself cannot read or write to those spaces of kernel memory. Unfortunately, as Meltdown demonstrates, Intel CPUs speculate past those protections, making that data obtainable by unauthorized actors.

218. Significantly, because of differences in AMD's (and other competitors') architecture and implementation of speculative execution, their CPUs are not vulnerable to Meltdown side-channel exploits. This is an issue exclusive to Intel's CPUs and stems from Intel's misplaced design decisions.

219. In order to mitigate Meltdown, Intel recommended that operating system developers implement *Kernel Page Table Isolation* ("KPTI"), which separates kernel and process page tables into two. As Intel knows, this separation has the effect of increasing the time it takes for instructions to be processed because the Translation Lookaside Buffer ("TLB") is flushed each time the OS kernel is involved and when control is transferred back to the user process. Thus, whereas a process may take eight CPU cycles to complete prior to Intel's recommended KPTI mitigation for Meltdown, that same process would take *26 times* that amount of time to complete the same process with Intel's KPTI mitigation.

5. "Foreshadow" or "L1 Terminal Fault"

220. In January 2018, a group of researchers discovered another exploit that takes advantage of both the Unauthorized Access and Incomplete Undo Defects inherent in Intel's CPUs as a result of Intel's flawed Intel's implementation of speculative execution. After the first variant (which targeted Intel's SGX technology) was identified, Intel's subsequent investigation uncovered two closely related exploit variants. The first variant has been dubbed "Foreshadow," and the latter two variants have been dubbed "Foreshadow-NG" (for "Next Generation") by researchers; Intel refers to the exploits collectively as L1 Terminal Fault (or "L1TF"). Like Meltdown, the Foreshadow exploits are based on the fact that Intel CPUs execute speculatively and defer

permission checks thereby creating a window of time during which an unauthorized process can steal sensitive information.

221. **Relevant Computer Architecture Background.** The L1 (level 1) data cache is a memory resource shared between all software running on the same core. Therefore, the ability to speculatively access data left in the L1 cache can have serious security consequences. Even worse, modern Intel processors with Hyper-Threading also share the L1 cache between sibling cores. As alleged more fully below, disabling Hyper-Threading is one necessary mitigation for government and commercial enterprise servers and cloud services using Intel CPUs.

222. Generally, and as discussed previously, to achieve a secure computer system, each process has its own separate virtual address space. When a process accesses a memory location in its virtual address space, the hardware translates the address into the corresponding physical address. One process should not be able to access another process's physical address space (unless the two processes are explicitly sharing data, e.g., to communicate with one another). The operating system keeps track of data access permissions by mapping virtual to physical addresses through page tables. The page tables are used to translate each process's virtual addresses to the physical addresses corresponding to its memory locations.

223. During a page table check or "walk," the CPU will perform the translation and will also check whether the page is actually "present" in main memory. Non-present entries can exist when a virtual page that has not been used recently is "swapped" or moved out to disk and the corresponding page table entry is then marked to show that process's page is not present. When access to that absent memory location is requested, a page fault (a type of exception) will occur, which will cause the address translation process to terminate, and the missing data must be located on disk and pulled back into physical memory.

224. But to speed performance, Intel CPUs continue to speculate forward and allow instructions to execute despite the page fault. Specifically, Intel CPUs are designed so that if the address translation process is prematurely terminated through a page fault, the L1 cache lookup is still performed based on the physical address pointed to in the page table (which is no longer the physical memory of the requesting process). This enables speculative instructions, that do not otherwise have the requisite permissions, to gain unauthorized access to data stored in the cache. The Foreshadow exploits are also referred to as "L1 terminal fault" because they cause the translation process to prematurely terminate through a page fault, while, dangerously, data is still being passed from the L1 cache to subsequent instructions.

225. Finally, as with Meltdown, unauthorized users can use the "Flush+Reload" technique to establish the secret information.

226. **Foreshadow-OS (CVE-2018-3620).** This variant allows an unprivileged application to access kernel memory. An unauthorized application can simply wait for the OS to clear the "present" bit in a page table entry (which happens when a memory page that has not been used recently is swapped out of memory to disk). The unauthorized actor then inputs a virtual address, which must be translated through the page table. Since the bit is marked not present in the page table, the translation process is terminated. Because of Intel's implementation of speculative execution, the unauthorized actor can then use speculative instructions to read any cached contents pointed to by the physical address from the page table entry.

227. **Foreshadow-VMM (CVE-2018-3646).** In a "virtualized" environment, where multiple guest operating systems run on the same machine, (e.g. cloud computing), the mapping and translation process is slightly modified. The Foreshadow-VMM variant allows an unauthorized

guest virtual machine to access memory belonging to other guest virtual machines and the hypervisor (which is the software that manages the virtualized environment).

228. In a virtualized environment, two translations may occur by using "extended" page tables. First, the guest machine's virtual address is translated to a guest "physical" address through its guest page table. Second, the guest "physical" address is translated to the underlying machine's host-physical address using the host page table.

229. An unauthorized guest has control over the guest page table and therefore can directly clear the "present" bit in that page table. That triggers the page fault, which terminates the translation process, eliminating the host address translation step. Due to Intel's flawed implementation of speculative execution, it is the guest "physical" address that is passed to the L1 data cache. Notably, because in this variant the guest has control over the guest page table and thus controls the "physical" address, the unauthorized guest can speculatively read any cached memory, including secret data belonging to other virtual machines or the hypervisor itself.[82]

230. **Foreshadow-SGX (CVE-2018-3615).** Intel's Software Guard eXtensions ("SGX"), introduced in 2013, allow users to allocate private regions of memory called "enclaves," which are intended to allow secure execution on an adversary-controlled machine. With SGX, an additional level of checks is supposed to be performed after the address translation process is completed in order to enforce strict access control for enclaves. In the SGX variant, unauthorized users can exploit the L1TF behavior described above to terminate the address translation process so that any

[82] Whereas the Meltdown attack described above was limited to reading privileged supervisor data mapped within an unauthorized user's virtual address space, the Foreshadow-type attacks directly expose cached physical memory contents to unauthorized actors from locations that are not mapped in the a unauthorized user's physical address space.

cached enclave secrets are passed to speculative instructions before SGX protections are enforced. Additionally, as with Meltdown, unauthorized users can leverage the TSX exception suppression "feature" to carry out the exploit.

231. Ironically, although Intel stated that SGX was "designed to increase the security of application code and data," *see* https://software.intel.com/en-us/sgx, SGX is itself vulnerable to the Foreshadow side-channel exploits. *See* https://arxiv.org/pdf/1709.09917.pdf.

232. As with Meltdown, AMD's and other competitors' CPUs are not vulnerable to Foreshadow side-channel exploits. Foreshadow is exclusively an Intel CPU problem and the result of Intel's flawed implementation of speculative execution.

233. In order to prevent Foreshadow exploits on Intel's defective CPUs, Intel must redesign its CPU hardware to eliminate the Defects. Short of that, mitigating Foreshadow requires: (a) OS modification of page table entry of not present pages to refer to invalid addresses, and (b) Intel's removal of microcode from the L1 data cache during privilege transitions. These mitigations increase L1 data cache misses, slowing the processor down.

234. In addition, for commercial and government enterprise servers and cloud services (e.g., Amazon Web Services, also known as "AWS") using Intel's processors, Foreshadow mitigations require the complete disabling of Hyper-Threading. Without Hyper-Threading, CPU cores are no longer shared between processes which results in a substantial degradation of performance.

6. SwapGS

235. In 2018, researchers revealed SwapGS (CVE-2019-1125). Researchers first alerted Intel to this exploit on August 7, 2018. Intel initially responded that it was already aware of the SwapGS exploit but did not intend to do anything to address it in affected CPUs. The researchers

who had discovered SwapGS continued to insist that the SwapGS exploit was problematic and, on March 29, 2019, provided an additional concern – a SwapGS exploit could be used to leak kernel memory. The existence of the SwapGS exploit was not disclosed publicly until August 6, 2019 – nearly a year from the date Intel was first made aware of its existence.

236. **Relevant Computer Architecture Background**. Intel processors have special instructions to allow a program fast access to data structures that support concurrent execution within the CPU and switching between tasks executing on the CPU. One of these instructions, SwapGS, from which the exploit derives its name, facilitates the fast switching between kernel mode and user mode. Depending on the particular special instruction utilized by the unauthorized user, a SwapGS exploit can leak data from the FS or GS registers. A "register" is a quickly accessible memory location within a CPU, consisting of a small amount of fast storage.

237. Utilizing the SwapGS exploit, an unauthorized user can take advantage of the Intel-designed speculative execution process to allow an unauthorized process to leak stale data from another process maintained in the FS or GS registers. Specifically, the unauthorized user starts by launching a "speculative segment write," by writing data to either the FS or GS register in the wrong format. The incorrect format will cause the unauthorized user program to be aborted triggering a fault. Due to Intel's defective design (Unauthorized Access), however, this will create a window in time during which the unauthorized user may read data maintained the FS or GS registers to which the unauthorized user otherwise would not have permission to access. These unauthorized accesses can be exploited in a manner similar to the Meltdown and Foreshadow exploits. Because, however, the patches for Meltdown and Foreshadow do not fix the root cause for generating the fault or assist (Unauthorized Access), the patches for Meltdown and Foreshadow do not affect an unauthorized user's ability to launch this kind of SwapGS exploit.

238. Because the SwapGS exploit leaks data stored in general use registers, the data stored there could be virtually anything stored in the CPU or memory, including kernel memory. This data can then be leaked from the CPU (Incomplete Undo) through a flush+reload attack.

239. There also is a version of the SwapGS exploit that involves the use of branch prediction to leak information from the kernel space. This form of the SwapGS exploit is similar to certain Spectre variants that exploit intentional branch (mis) prediction to trick the kernel into leaking data. Despite these similarities, however, the patches for Spectre do not stop an unauthorized user from launching this kind of SwapGS exploit.

240. It is reported that only Intel-designed CPUs are susceptible to a SwapGS exploit.

7. MDS Exploits

241. In 2018, researchers revealed a new series of exploits, dubbed by Intel as microarchitectural data sampling or MDS exploits. MDS exploits "leak arbitrary data across address spaces and privilege boundaries (e.g., process, kernel, SGX, and even CPU-internal operations)," each of which exploits Intel's proprietary implementation of speculative execution.[83] These exploits are "powerful." Researchers alerted Intel to key aspects of what became known as Microarchitectural Data Sampling Uncacheable Memory ("MDSUM") (CVE-2019-11091), as early as March 28, 2018.[84]

242. Subsequent discoveries both within Intel and by independent researchers led to the identification of multiple MDS exploits, including Microarchitectural Fill Buffer Data Sampling

[83] Stephan van Schaik *et al.*, *RIDL: Rogue In-Flight Data Load*, at 1 (2019, updated Jan. 27, 2020), https://mdsattacks.com/files/ridl.pdf.

[84] Michael Schwarz *et al.*, *ZombieLoad: Cross-Privilege-Boundary Data Sampling* (2019), https://zombieloadattack.com/zombieload.pdf.

("MFBDS") (CVE-2018-12130), Microarchitectural Load Port Data Sampling ("MLPDS') (CVE-2018-12127), and Microarchitectural Store Buffer Data Sampling ("MSBDS") (CVE-2018-12126) in June 2018,[85] Transactional Synchronization Extensions Asynchronous Abort ("TAA") (CVE-2019-11135) in September 2018,[86] L1D Eviction Sampling ("L1DES") (CVE-2020-0549) in April 2019,[87] and Vector Register Sampling ("VRS") (CVE-2020-0548) in October 2019.[88]

243. Researchers consider the implications of MDS exploits "worrisome" because, among other things, these exploits "bypass[] all existing 'spot' mitigations [i.e., patches] in software . . . and hardware . . . and cannot easily be mitigated even by more heavyweight defenses."[89] Indeed, MDS exploits likely ensure that "spot" mitigations, such as those employed by Intel and software companies, are not "sustainab[le]" as new forms are revealed, and that more "fundamental mitigations are needed to contain ever-emerging speculative execution attacks."[90]

244. As in the case of the discovery of Meltdown, Foreshadow, and Spectre, though, Intel again embargoed information, which prevented disclosure about these attacks for significant periods of time. Consequently, the MDS exploits were disclosed on May 15, 2019 (MDSUM, MFBDS, MLPDS, and MSBDS), November 12, 2019 (TAA), and January 27, 2020 (L1DES and VRS).

---

[85] Intel registered each of these exploits with the CVE database on June 11, 2018. However, this date "[t]his date does not indicate when the vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE." *See* https://cve.mitre.org/about/faqs.html#date_entry_created_in_cve_entry (last accessed April 26, 2020).

[86] Researchers reported the TAA exploit to Intel on September 29, 2018.

[87] Researchers reported L1DES exploit to Intel on April 24, 2019.

[88] Researchers reported VRS exploit to Intel on October 1, 2019.

[89] Stephan van Schaik, et al., *RIDL: Rogue In-Flight Data Load*, at 1, https://mdsattacks.com/files/ridl.pdf (last visited Apr. 6, 2020).

[90] *Id.* at 1.

Researchers were not allowed to disclose TAA until November 12, 2019, despite Intel having been provided proof of TAA in September 2018.

245. The MDS exploits have a variety of nicknames generated by the researchers who have publicly reported them: RIDL (Rogue Inflight Data Load), ZombieLoad, Fallout, and Cacheout. The team that publicly reported and named RIDL reports that all of the MDS exploits, including Zombieload, Fallout, and Cacheout, are variants of RIDL. These researchers named these exploits "RIDL" because the source of the leakage of in-flight data was, at first, a mystery or riddle, and to acknowledge that the RIDL exploits follow Meltdown, which Intel formally named RCDL or rogue data cached load.

246. The team that discovered Zombieload attaches that moniker to the following MDS exploits (each of which also are claimed variants of RIDL): MFBDS (CVE-2018-12130), TAA (CVE-2019-11135), and LIDES (CVE-2020-0549). Zombieload refers to the speculatively executed loads that are a hallmark of these exploits, which resurrect decarded in-flight data, and the fact that the exploit is difficult to "kill."

247. The researchers that identified MSBDS (CVE-2018-12126) dubbed it "Fallout" because this exploit is the direct consequence of the Meltdown exploit and fallouts are typically the results of meltdowns. Moreover, like the Meltdown exploit, Fallout requires "software fixes with potentially significant performance overheads are still necessary to ensure proper isolation between the kernel and user space."[91]

[91] Claudio Canella *et al*., *Fallout: Leaking Data on Meltdown-resistant CPUs*, at 1, https://mdsattacks.com/files/fallout.pdf (last visited Apr. 6, 2020).

248. The researchers that identified LIDES (CVE-2020-0549) dubbed it "Cacheout" because "cache" is a homophone for "cash" and the exploit allows the unauthorized user to force data out of the caches into a buffer and subsequently leak it.

249. **Relevant Computer Architecture Background**. While the Meltdown, Foreshadow, and Spectre exploits leak data stored in the CPU's caches, MDS exploits leak in-flight data. CPUs perform instructions as a series of steps. An instruction is said to have "committed" once all steps have been completed. While a CPU is processing an instruction, the data utilized by that instruction is "in-flight." Because CPU caches can perform only a few of the steps necessary to complete instructions each clock cycle, the CPU relies on a variety of "buffers" and "ports" within the CPU, including "line fill buffers," "load ports," and "store buffers" to temporarily hold in-flight data until the instruction that requires it has either been completed or cancelled.

250. The MDS exploits described below read unsecured "in-flight" data, as opposed to data stored in memory locations, and thus differ from Meltdown, Spectre, and Foreshadow. Further, because Intel has failed to fix the underlying undisclosed Defects (the root cause of the Intel CPU Exploits), none of the mitigations to combat the Meltdown, Spectre, and Foreshadow exploits prevent MDS exploits. In contrast, processors designed by Intel's competitors, including those designed by AMD, are immune to an MDS exploit, further confirming Intel's defective design choices.

251. **MFBDS (CVE-2018-12130)**. Intel's CPU design allows an unauthorized user to deploy the MFBDS exploit to leak data stored within the line fill buffers by inducing speculative execution. Specifically, Intel's design allows the line fill buffers to hold on to in-flight data even after they have been copied to their destination (e.g., the Level 1 cache). The stale in-flight data in the line fill buffers can be read by speculatively executed loads under conditions generated by an

unauthorized user. Intel's CPU design also allows data retrieved by one program to be read by another program from the line fill buffers without authorization.

252. In an MFBDS exploit, an unauthorized user first triggers a condition that causes repeated speculative execution within the CPU by generating exceptional events, including "faults" and assists." Because Intel's CPU design does not require any checks to determine whether a program has permission to access data in the event of a fault or an assist (Unauthorized Access), in-flight data temporarily stored within the line fill buffer can be "read" by the unauthorized user. Normally, programs need to have authorization to access data that is not theirs. By exploiting this vulnerability in Intel processors, unauthorized users can gain access to *any* data that is present in the line fill buffers, including data used by programs that they normally would not have access to. This data can include critical information such as passwords, cryptographic keys used for disk encryption or logins, browser history, browser authentication cookies, or other information that can aid or enhance other attack methods.

253. Once the in-flight data temporarily stored within the line fill buffer has been read by the unauthorized user, it can be leaked from the CPU utilizing a covert communication channel using the CPU's unsecured cache (Incomplete Undo) to leak the in-flight data, the most popular of which is the flush+reload method.

254. Because leaking in-flight data can quickly result in the extraction of voluminous data/information, the MFBDS exploit also employs a filtering technique to intelligently sample the in-flight data. This filtering technique allows the unauthorized user to look for a particular data sequence of interest, e.g., a user password that is stored in a file and leak that data.

255. According to AMD, the MFBDS exploit is not successful against its CPUs because AMD designed its processors to ensure that the translation lookaside buffer (or TLB) always checks

the permissions of speculatively executed loads to determine whether these loads should be given access to data in the fill buffer. Intel, however, sacrificed security and proper microarchitecture design by failing to enforce permission checks prior to speculative execution, and by failing to clear the line fill buffer once the data temporarily held within has been written to the data cache.

256. **MSBDS (CVE-2018-12126)**. Intel's CPU design allows an unauthorized user to deploy the MSBDS exploit to leak data stored within the "store buffers" by inducing speculative execution. Store buffers temporarily hold values before they are written to memory. A function of a store buffer is to "forward" data to memory locations when appropriate, i.e., when the requesting application has authorization to read the data maintained in the store buffer. Intel's CPU design allows the store buffers to forward data held therein without fully checking if the requesting application has the authorization to read that data (Unauthorized Access). This issue is compounded when the CPU is operated in hyperthreaded mode. In that instance, stale data from one thread maintained in the store buffers can be accessed by another thread that does not have permission to read that data.

257. The MSBDS exploit can be used against Intel-designed store buffers as described in ¶¶251-52 above. Effectively, the unauthorized user forces the CPU to engage in speculative execution leading to store-to-loading leakage. Because the Intel-designed CPU does not check the permissions of an application to access data within the store buffer once an assist or fault is generated (Unauthorized Access), an unauthorized user can access this data and then utilize a flush+reload exploit to leak out that information through the CPU's L1 cache (Incomplete Undo). With the MSBDS exploit, an unauthorized user can gain any information that is left over in the store buffers. Given that all data that is used for the "write" processing step goes through the store buffers of a

CPU, this essentially means that an unauthorized user can access *any* value written by a victim thread, including keys, secrets, passwords, and cookies.

258. The fact that an unauthorized user can access stale—but highly private and valuable—data left in the store buffers with MSBDS "has profound consequences for defenses, as merely draining outside stores by serializing the instruction stream . . . does not suffice to fully mitigate store buffer leakage."[92]

259. The MSBDS exploit does not work on AMD processors because AMD designed its processors to prevent an unauthorized application from reading data maintained in the store buffers when there is an assist or fault. In search of speed and marketing claims, Intel, however, deferred privilege checks when faced with an assist or fault, and further failed to clear out the store buffers of stale information. Implementing such steps—important elements of sound and secure microarchitecture design—would have jeopardized the performance claims that Intel chose to prioritize over security.

260. **MLPDS (CVE-2018-12127)**. Intel's CPU design allows an unauthorized user to deploy the MLPDS exploit to leak data stored within the buffers in the "load ports" by inducing speculative execution. Load ports are a set of wires that carry information across different blocks of the CPU. In a CPU, a load port holds results of "reads" from the data cache and the buffers in the load ports hold cache lines that are spilled from the L1 data cache.

261. Intel's load ports design allows the data maintained in these ports to be forwarded to speculatively executed instruction when there is a fault or an assist without first checking whether that instruction has permission to access the data within the load port (Unauthorized Access).

[92] Claudio Canella *et al.*, *Fallout: Leaking Data on Meltdown-resistant CPUs*, at 1, https://mdsattacks.com/files/fallout.pdf (last visited Apr. 6, 2020).

Specifically, the MLPDS exploit can be used against Intel-designed load ports as described in ¶¶251-52 above. Effectively, the unauthorized user forces the CPU to engage in speculative execution leading to faults or assists. Because the Intel-designed CPU does not check the permissions of an application to access data within the load port once the fault or assist is generated (Unauthorized Access), an unauthorized user can access this data and then utilize a flush+reload attack to leak out that information through the CPU's L1 cache (Incomplete Undo). With the MLPDS exploit, an unauthorized user can gain any information that is left over in the load ports. Notably, the MLPDS exploit does not work on AMD processors.

262. Through the use of sound and secure microarchitecture design, Intel could have prevented MLPDS exploits—i.e., by clearing the buffers in the load ports after they have been used or tagging the information held within the load buffers with ownership information that prevents data in the load port from being speculatively accessed across programs.

263. **MDSUM (CVE-2019-11091)**. Intel's CPU design allows an unauthorized user to deploy the MDSUM exploit to leak data, specifically, uncacheable data, stored within the "write buffers" by inducing speculative execution. Uncacheable data is any data that a programmer determines can be stored only in main memory, requiring it to bypass all caches when utilized by a CPU. Typically, data that is not frequently used by the program is deemed uncacheable and is not stored in cache to ensure that there is more space in the CPU's caches for data that is frequently utilized. Uncacheable data is maintained in temporary buffers until it can be written to memory.

264. The MDSUM exploit can be used against Intel-designed temporary buffers as described in in ¶¶251-52 above to access uncacheable data stored therein. Specifically, because the Intel-designed CPU does not check the permissions of an application to access uncacheable data within the temporary buffers once the fault or assist is generated (Unauthorized Access), an

unauthorized user can access this data and then utilize a flush+reload attack to leak out that information through the CPU's L1 cache (Incomplete Undo). Notably, the MDSUM exploit does not work on AMD processors.

265. **TAA (CVE-2019-11135)**. The TAA exploit takes advantage of one of Intel's proprietary TSX hardware feature to efficiently mount an MDS exploit even on allegedly non-vulnerable Intel CPUs (e.g., CPUs with hardware mitigations meant to address MDS exploits). According to Intel, "[t]he [TAA] vulnerability affects the same microarchitectural structures as [the] MDS [exploits] but uses a different mechanism for the exploit."[93]

266. TSX refers to an Intel-specific set of instructions for its CPUs which, when implemented, are meant to improve the performance of parallel programs on the same CPU. Specifically, TSX are transactional memory instructions that allow a programmer to group together a set of instructions to execute in an all or nothing manner when programming an application. If there is an interruption while this set of instructions is executing, the transaction (i.e., the set of instructions set to execute together), is aborted and retried at a later time. This abort-and-retry mechanism is automatically performed by the hardware due to TSX and is unique to Intel CPUs.

267. Intel's TSX allows an unauthorized user to exploit both the Unauthorized Access and Incomplete Undo Defects to read secret "in-flight" data by using an "abort and retry" mechanism to create a window of time during which data can be read from many intermediate CPU buffers, including the line fill buffer. Specifically, an unauthorized person creates a transaction, which is then intentionally aborted by flushing the cache to a particular memory address (i.e., a Flush +

[93] *Side Channel Vulnerabilities: Microarchitectural Data Sampling and Transactional Asynchronous Abort*, Intel, https://www.intel.com/content/www/us/en/architecture-and-technology/mds.html (last visited Apr. 28, 2020).

Reload side-channel attack). The flushed instruction from the cache then allocates space in the line fill buffer, allowing the transaction to speculatively access the data in the fill buffer. Put simply, the TAA exploit allows old (yet still private) data from the line fill buffer containing sensitive information to be read by the unauthorized transaction.

268. As with other MDS exploits, the TAA exploit allows an unauthorized user to exploit Intel's CPU defective design choices to gain access to virtually ***any*** data present in the line fill buffers of the CPU, including data used by programs the unauthorized person would ordinarily have no access to and, most critically, data such as passwords, cryptographic keys used for disk encryption and logins, browser history, and browser authentication cookies. To be sure, one researcher took just 30 seconds to use TAA to trick a target machine into revealing a hash of an administrator's password.[94]

269. Indeed, in order to protect Intel's CPUs from the TAA exploit, it is recommended that two of the important components and marketing features of Intel's CPUs – Hyperthreading (SMT) and TSX – be completely disabled, which are used to, among other things, speed up execution of multi-threaded software and make parallel programming easier. Critically, the TAA exploit does not impact AMD processors because AMD processors do not have TSX instructions implemented in them.

270. **VRS (CVE-2020-0548)**. Intel's CPU design allows an unauthorized user to deploy the VRS exploit to leak in-flight data stored within the CPU's vector registers after certain operations are completed. Like buffers and ports, registers are data holding locations within the CPU that maintain in-flight data, specifically operands used for operations or results of the

[94]Andy Greenberg, *Intel Failed to Fix a Hackable Chip Flaw Despite a Year of Warnings*, WIRED (Nov. 12, 2019), https://www.wired.com/story/intel-mds-attack-taa/

operations. Vector instructions, i.e., program instructions that require the CPU to employ the vector registers to complete an operation, are used to speed up rendering graphics, to efficiently process strings of text, or to efficiently perform complicated cryptographic operations.

271. The VRS exploit allows an unauthorized user to gain access to sensitive information in a CPU's registers by executing speculative code that moves data in the vector register into the CPU's memory. While "in-flight," from the vector register to the CPU's memory, the data is maintained in the store buffer. The VRS exploit then removes the data from the store buffer using TSX instructions. This exploit can then be used against Intel designed store buffers as described in ¶¶251-52. Notably, the VRS exploit has been reported in Intel CPUs with microcode patches to address the Fallout exploit, demonstrating that those mitigations were insufficient to address the undisclosed Defects in Intel's CPU design.

272. **L1DES (CVE-2020-0549)**. Intel's CPU design allows unauthorized users to utilize the L1DES exploit to push data within the L1 data cache into one of the CPU buffers and leak that data through the use of speculative execution. Specifically, the L1DES exploit takes advantage of TSX instructions—proprietary Intel instructions—to position cached data into a buffer and leak it through an MDS exploit, as described above in ¶¶251-52.

273. The L1DES exploit demonstrated that Intel's mitigation plan for other MDS exploits was incomplete because, even with those mitigations, researchers were able to force a victim's sensitive data out of the L1 data cache into the microarchitectural buffers after the operating system clears them, which could then be leaked to obtain the victim's data utilizing the L1DES exploit. In order to mitigate the L1DES exploit, it is necessary both to overwrite the buffers and to flush the L1 data cache in the CPU before switching across security domains (or in many cases, between the operating system and a virtual machine), which materially degrades CPU performance. Because

L1DES exploits Intel's defective CPU design, as well as its proprietary TSX instruction set, L1DES does not impact AMD CPUs. Notably, this exploit has been reported in Intel processors with microcode patches meant to fix the original RIDL and Zombieload variants, demonstrating that those mitigations were insufficient to address Intel's defective CPU design.

274. **Snoop Assisted L1D Sampling (CVE-2020-0550)**. Intel's CPU design allows an unauthorized user to deploy the Snoop Assisted L1D Sampling to push data from Intel's L1 data cache into a buffer via a TSX instruction which, as designed by Intel, is vulnerable to an MDS exploit.

275. Bus "snooping" or "monitoring" refers to a "cache-coherence mechanism" used by the CPU to ensure the "coherence" of information stored in a variety of caches, particularly when a CPU is used for multi-threaded, parallel applications. Having multiple copies of shared information within the CPUs caches improves the overall performance of the processor; this information, however, must be the same in each cache. To ensure this "coherence," caches are accessed via a microarchitectural element that is shared among the systems—a "bus connection"—which is then monitored by cache controllers to ensure that the consistency of the copied data across the CPU's caches. For instance, if a transaction modifies the memory location used by one of these copies, the bus will share that information with each cache so that the copied data is updated, and coherence is maintained.

276. With a Snoop-assisted L1D sampling exploit, an unauthorized user utilizes a version of the TAA exploit to push data from the L1 data cache into the CPU buffers where it is then vulnerable to an MDS exploit as described in ¶¶251-52 above. Importantly, Intel has advised OS developers that "Snoop-assisted L1D sampling could be mitigated by flushing the L1D cache before executing potentially unauthorized applications, which would require changes to the OS scheduler

when hyperthreading is enabled and could impact the performance of system transitions."[95] AMD processors are not impacted by Snoop-assisted L1D.

277. **Load Value Injection (CVE-2020-0551)**. The LVI exploit utilizes in-flight data obtained during an MDS exploit to trick an Intel-designed CPU to turn on itself and leak its privileged data during a fault or assist generated by speculatively executed instructions (Unauthorized Access and Incomplete Undo)

278. There are at least two variants of the Load Value Injection exploit: LVI Stale Data and LVI Zero Data. LVI Stale Data takes advantage of stale in-flight data within the buffers and LVI Zero Data takes advantage of the mitigation for Meltdown and Foreshadow that inserts a 0 value when there is a fault or assist during speculative execution. In other words, a mitigation for certain aspects of the Unauthorized Access Defect has exposed Intel-designed CPUs to LVI exploits, demonstrating that these mitigations were insufficient to fix the undisclosed Defects in Intel's CPU design.

8. "Spectre"

279. Beginning in April 2017, researchers discovered the first in a series of related security exploits or exploits known as Spectre. Spectre gets its name from "speculative execution." Intel was aware of the first two Spectre variants by June 1, 2017, but the public did not become aware of Spectre or the security vulnerability that it exploited until January 3, 2018.

280. Generally speaking, a Spectre exploit takes advantage of the security vulnerabilities created by Intel's reliance upon speculative execution and, in particular, the branch prediction unit,

---

95 *Snoop-assisted L1 Data Sampling / CVE-2020-0550 / INTEL-SA-00330* https://software.intel.com/security-software-guidance/software-guidance/snoop-assisted-l1-data-sampling (last visited Apr. 28, 2020).

and an unsecured cache subsystem to achieve increased performance. Spectre allows unauthorized users to gain access to memory locations but only within the same process (e.g., another tab in a web browser). But unlike Meltdown and Foreshadow, the Spectre exploit uses Intel CPUs' branch predictor to enable the unauthorized access.

281. Spectre trains the branch predictor to make a wrong prediction. Critically, it is difficult to detect the execution of a Spectre exploit, in part because the CPU does not recognize that its "mis-speculation" was, in fact, coerced, and cache-timing side-channel exploits generally leave no readily discernible trail to indicate that the caches have been improperly accessed. Thus, the unauthorized user can compromise Intel's CPU and obtain sensitive information without leaving any "fingerprints" behind.

282. Each Spectre exploit involves several steps. First, the unauthorized user uses a "leak gadget" to coerce the CPU to speculatively execute instructions that are not a normal part of the processor's operation. Second, unaware that it is under attack, Intel's CPU fetches and stores within its caches the data needed to execute the coerced instructions. Third, still unaware that it is under attack, Intel's CPU determines that it has "mis-speculated," or speculatively executed incorrect instructions, and proceeds to flush its pipelines—*but not its caches*—of the effects of the incorrect instructions. Finally, the unauthorized user uses a "transmit gadget" to execute an exploit on Intel CPU's caches and surreptitiously transmit the information that remains after the processor's mis-speculation. By July 10, 2018, researchers had identified six Spectre variant exploits as follows:

Name of Variant	**Date 1st Identified**	**Date 1st Reported**	**Key Attributes of Variant**
Variant 1, Bounds Check Bypass (CVE-2017-5753)	June 2017	1/3/2018	Exploits the speculative operations that occur when CPUs execute certain conditional branch instruction—e.g., whether an input is "in bounds"—to engage in otherwise unauthorized or unnecessary memory accesses.
Variant 1.1, Bounds Check Bypass on Loads (CVE-2018-3693)		7/10/2018	Exploits speculative stores and how the CPU addresses speculative buffer overflows to bypass mitigations implemented for earlier Spectre variants. This variant uses a form of "stack smashing," a common method of capitalizing on a buffer overflow.
Variant 1.2, Read-only Protection Bypass		7/10/2018	Exploits speculative stores and how the CPU addresses speculative buffer overflows where the processor doesn't enforce read/write protections to bypass mitigations implemented for earlier Spectre variants.
Variant 2, Branch Target Injection (CVE-2017-5715)	June 2017	1/3/2018	Exploits the part of the CPU that directs what operations need to be speculatively executed (the "indirect branch predictor") to allow unauthorized code to be speculatively executed.
Variant 3a, Rogue System Register Read (CVE-2018-3640)		5/23/2018	Exploits the "read system register" function to allow an unauthorized user to improperly access information about the state of the CPU's system register (similar to a cache).
Variant 4, Speculative Store Bypass (CVE-2018-3639)		5/23/2018	Exploits the CPU's ability to speculatively load data into its caches.

283. On July 23, 2018, a team of security experts from the University of California, Riverside disclosed a new Spectre exploit, SpectreRSB.[96] In a SpectreRSB exploit, an unauthorized

[96] E.M. Koruyeh, *et al.*¸*Spectre Returns! Speculation Attacks using the Return Stack Buffer* https://arxiv.org/pdf/1807.07940.pdf (last visited May 10, 2020).

user exploits a different component of Intel's CPU microarchitecture utilized in speculative execution—the return stack buffer or RSB. The purpose of an RSB in a processor employing speculative execution is to predict where Intel's CPU should go to, or the "return address," once its current operation is complete. Like the other variants of Spectre, SpectreRSB involves utilizing a "leak gadget" to "poison" the RSB, which has the effect of either mis-training or "polluting" the branch prediction unit so as to force it to speculatively execute certain instructions.

C. Intel Was Aware of Numerous Methods That Would Have Mitigated Side-Channel Exploits

284. Intel at all times treated (and continues to treat) its CPU design files as highly confidential trade secrets and does not disclose such information to consumers. Plaintiffs and members of the Class did not have access to Intel's proprietary chip and microarchitecture designs, and thus could not reasonably discover the Defects on their own.

285. At all relevant times, Intel has had exclusive knowledge concerning its defective hardware design that deferred privilege checks and permitted unauthorized memory access, thus compromising security.

286. But, as many of its patent filings show, Intel was fully aware of the vulnerability of its architecture to side-channel exploits and the steps it could have taken to plug the security holes in its leaky microarchitecture and architecture design. In addition, Intel was aware of many research papers that proposed various solutions to issues with speculative execution generally, but it did nothing.

287. As previously discussed, Intel had previously implemented safeguards in its P6 architecture that would have largely protected against the Intel CPU Exploits. That is why AMD's CPUs are reported to be immune from all of the aforementioned exploits, except for Spectre. Unlike

Intel, AMD did not remove well-accepted security. Thus, to fix the Unauthorized Access Defect, Intel would need to disable hardware that allows transient instructions to receive unauthorized data (e.g., return a dummy value such as 0 or a random number)—which is what AMD CPUs do and what Intel's earlier P6 architecture did.

288. Intel knew that its CPUs left data insecure and thus vulnerable to exploit. It failed to disclose that, in designing its CPUs, it had sacrificed security for speed and specifically chose to allow unauthorized access to users' privileged data—all in an effort to secure a performance advantage over AMD and other competitors.

289. As previously discussed, side-channel exploits, such as the Intel CPU Exploits, require fine-grain time measurements to time cache accesses to leak information. Intel includes in the x86 Instruction Set a Read Time-Stamp Counter instruction (or RDTSC), which provides high resolution CPU timing information. RDTSC is the instruction used to collect timing information in virtually all cache side-channel exploits.

290. In the '294 patent, Intel recognized the role that RDTSC played in cache side-channel exploits. In particular, Intel acknowledged that "[d]isabling counters almost guarantees that timing-based attacks cannot be executed by Ring 3 [user privilege level] spies." *Id*. at col. 3, l. 14-15. Intel then proposed limiting access to the RDTSC instruction based on privilege, "leaving it to the OS [operating system] to determine which applications have the privilege to read timestamp and performance counters." *Id*. at col. 4, l. 19-20.

291. Furthermore, in 2012, Intel was presented with a solution that further restricted access to the fine-grain timekeeping needed to carry out timing side-channel exploits. In Martin *et al.*, *Timewarp: Rethinking Timekeeping and Performance Monitoring Mechanisms to Mitigate Side-Channel Attacks* (2012), the authors provided a comprehensive solution that would "limit the fidelity

of fine grain timekeeping and performance counters, making it difficult for an unauthorized user to distinguish between different microarchitectural events, thus thwarting attacks." *Id*. at Abstract.

292. Intel has proposed other protections to prevent cache side-channel exploits. In the '356 patent, Intel described a scenario that again foreshadows the exploits at issue here and noted that to thwart such an exploit, one could prevent repeated evictions from the cache of the victim's data, which is a critical step used in cache side-channel exploits.[97] Intel went on to propose a protected cache design in which a cache controller handles access to, and eviction of, given cache line data based on protection data stored in the cache that controls access to the corresponding cache line.

293. Another mitigation that Intel was aware of from at least 2010[98] are the cache designs presented by Dr. Lee in Lee *et al.*, *New cache Designs for Thwarting Software Cache-based Side Channel Attacks* (2007). Dr. Lee proposed a cache design that "can defend against cache-based side channel attacks . . . with very little performance degradation and hardware cost." Her cache design incorporates a cache partition mechanism, called PLcache, that creates "a flexible 'private partition'" so that "cache lines cannot be evicted by other cache accesses not belonging to this private partition." *Id.* at 4.1. Dr. Lee also a described a cache design, called RPcache, which

[97] In the described attack, two threads use the same cache such that "when the attacker program is swapped into the processor state in place of the victim program, the data of the victim program in the cache is evicted and vice-versa. [W]hen the attacker program is being swapped in again, it can identify which parts of its own data was evicted by observing the latency of its read operations. By repeating that process, the attacker can infer information about the access patterns of the victim and expose a private key associated with the victim program, thus enabling the attacker program to access the private data of the victim." '356 patent at col.2, l.9-19.

[98] Intel participated in the Hot Chips 26 conference where Dr. Lee presented her cache design. *See Hot Chips: A Symposium on High Performance Chips* (Aug. 10-12, 2014) https://www.hotchips.org/archives/2010s/hc26/ (last visited May 5, 2020).

employs dynamic random mapping to deny an unauthorized user information about where potential victim code exists in the cache. *Id.* at 4.2. [99]

294. In sum, Intel was fully aware that its leaky cache design posed a substantial security risk from increasingly effective side-channel exploits. Though Intel was aware of techniques or designs that could mitigate or thwart variants of such exploits. Intel failed to do so.

295. It was only after Meltdown and Spectre were disclosed, and it had a proverbial "gun to its head," that Intel acquiesced to prospectively change its hardware design to deal with vulnerabilities inherent to its defective design.

296. Even then, however, Intel failed to fix the underlying Defects in its CPU design that allowed the authorized memory access, and as a result numerous additional exploits were disclosed on an ongoing basis for over two years since, with the most recent one found in March 2020.

D. <u>The Intel CPU Exploits Are Both Weaponized And Untraceable.</u>

297. The Intel CPU Exploits are not merely theoretical threats. They are real-world threats that are weaponized "in the wild."

298. As of January 30, 2018, Fortinet, a prominent manufacturer of enterprise network hardware, reported that it had found dozens of malware samples that have started taking advantage of the proof-of-concept codes for Meltdown and Spectre. In the span of two weeks after the vulnerabilities were disclosed, security research teams found 119 malware samples associated with

[99] Dr. Lee has received a patent, *Cache Memory Having Enhanced Performance And Security Features*, U.S. 8,549,208, issued Oct. 1, 2013 and published Jul 15, 2010, that describes her secure cache design. She also filed a patent application, *Systems and Methods for Random Fill Caching and Prefetching for Secure Cache Memories*, Pub. No. U.S. 2016/0170889 A1 (filed Dec. 14, 2015), that proposes additional security enhancements.

Meltdown and Spectre. After analyzing the samples, Fortinet discovered they were all based on the previously released proof of concept.[100]

299. As of February 1, 2018, the number had grown to 139 malware samples.[101]

300. Alex Ionescu, a security architect and consultant expert in kernel development, security training, and reverse engineering at CrowdStrike, Inc., confirmed in a tweet that he had "weaponized" Meltdown.[102]

301. Even Intel admitted that the Intel CPU Exploits can "be maliciously exploited in the wild by highly sophisticated cyber-criminals."[103]

302. The Intel CPU Exploits "leave[] no trace that would make in-the-wild attacks detectable."[104] The well-known cybersecurity company McAfee advised that the Intel CPU Exploits

[100] *See Meltdown/Spectre Update*, Fortinet (Jan. 30, 2018), https://www.fortinet.com/blog/threat-research/the-exponential-growth-of-detected-malware-targeted-at-meltdown-and-spectre.html ; *see also* Lucian Armasu, *Hundreds of Meltdown, Spectre Malware Samples Found in the Wild*, Toms Hardware (Feb. 1, 2018) https://www.tomshardware.com/news/meltdown-spectre-malware-found-fortinet,36439.html .

[101] *See* Andy Patrizio, *Researchers find malware samples that exploit Meltdown and Spectre*, NetworkWorld.com (Feb. 8, 2018), https://www.networkworld.com/article/3253898/researchers-find-malware-samples-that-exploit-meltdown-and-spectre.html .

[102] *See* @aionescu, Twitter (Jan. 10, 2018, 8:59 PM), https://twitter.com/aionescu/status/951272403853717504 (last visited May 5, 2020).

[103] Maxwell Cooter, *We've secured our CPU silicon, and ready to secure your business, says post-Meltdown Inte*", The Register (Sept. 12, 2019), https://www.theregister.co.uk/2019/09/12/securing_the_silicon/.

[104] Andy Greenberg, *Intel is Patching the Patch for the Patch for Its 'Zombieload' Flaw*, Wired (Jan. 27, 2020), https://www.wired.com/story/intel-zombieload-third-patch-speculative-execution/.

"are exceptionally hard to detect as they do not leave forensic trace or halt program execution. This makes post-infection investigations and attack attribution much more complex."[105]

E. The Intel CPU Exploits Are An Intel Problem; Not An Industry-Wide Problem.

303. Only Intel implemented the flawed CPU microarchitecture and architecture, including both Defects (Unauthorized Access and Incomplete Undo).

304. AMD does not appear to be vulnerable to the vast majority of Intel CPU Exploits. As noted, the Intel CPUs at issue are subject to a large number of the Intel CPU Exploits and related variants (see chart at Paragraph 318 below); whereas the CPUs manufactured by Intel's principal competitor, AMD, are at risk of only Spectre.

305. In the face of this reality, Intel has continued to mischaracterize the exploits as an industry-wide problem. For example, in response to story by Computer Business Review, which reported that the Intel CPU Exploit SWAPGS bypasses all known mitigation mechanisms implemented in the wake of the disclosure of Meltdown and Spectre, "Intel's US PR agency told Computer Business Review in an email that this is 'not an Intel-specific issue. We would appreciate if you could update your article to note that this is an industry-wide issue that affects both Intel and AMD.'"

306. In response to Intel's email, Computer Business Review contacted AMD. "AMD reject[ed] that claim, saying 'based on external and internal analysis, AMD believes it is not vulnerable to the SWAPGS variant exploits because AMD products are designed not to speculate on the new GS value following a speculative SWAPGS. For the exploit that is not a SWAPGS

[105] *See Decyphering the Noise Around 'Meltdown' and 'Spectre'*, McAfee Advanced Threat Research (Jan. 4, 2018), https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/decyphering-the-noise-around-meltdown-and-spectre/.

variant, the mitigation is to implement our existing recommendations for Spectre variant 1.' (i.e., no new mitigations have been required.)."

307. In short, in side by side safety analyses between Intel and AMD processors, industry experts have concluded that AMD's CPUs are safer and more secure than Intel's CPUs. It is reported that, consistent with sound CPU microarchitecture and architecture design principles, AMD—unlike Intel—designed its CPUs with security in mind.[106]

308. As a result, AMD has been "outselling Intel in the desktop category with its third-generation Ryzen processors. Intel is stumbling, rushing out new processors, slashing prices by as much as half, and struggling to work out how to compete against AMD[.]'"[107]

309. Indeed, it has been reported that numerous OEM and cloud providers have transitioned from systems employing Intel processors to those powered by AMD processors. Following Google's Project Zero security team's disclosures concerning the Meltdown and Spectre CPU exploits, Google has reportedly grown increasingly dissatisfied with Intel's processors.[108]

---

[106] Lucian Armasu, *Intel vs AMD Processor Security: Who Makes the Safest CPUs?*, Tom's Hardware (Nov. 4, 2019), https://www.tomshardware.com/features/intel-amd-most-secure-processors.

[107] Rich Edmonds and Richard Devine, *Intel spent much of this decade all alone churning out mino CPU upgrades, but we take a look at how AMD managed to claw its way back onto the field*, Windows Central (Dec. 23, 2019), https://www.windowscentral.com/decade-in-review-amd-ryzen-intel-2010s; see also https://www.techspot.com/news/80614-report-intel-cut-desktop-cpu-prices-10-15.html

[108] Lucian Armasu, *AMD's Epyc Potential Win: Google May Ditch Intel*, Tom's Hardware (July 30, 2019), https://www.tomshardware.com/news/google-switch-intel-server-cpus-amd-epyc,40045.html.

Google confirmed the rumors and announced it was moving to systems powered by AMD processors for internal workloads as well as for Google Cloud customers.[109]

310. At the same time, Twitter confirmed it was moving to AMD-powered computing systems for its data centers as well.[110]

311. Backblaze has also stated it may move to AMD-powered systems.[111] This news comes after Backblaze openly said that Meltdown and Spectre were causing them to consider alternatives to Intel-powered systems.[112]

312. The switch to AMD CPUs is not limited to cloud services. Among others, Microsoft announced plans to use AMD processors instead of Intel processors for its upcoming Surface laptop line.[113]

313. In addition to placing its financial interests ahead of the best interests of its customers, Intel placed its interests ahead of national security. Notably, although it notified a group

---

[109] Bart Sano and Brad Calder, *AMD EPYC processors come to Google- and to Google Cloud* Google Cloud (Aug. 7, 2019), https://cloud.google.com/blog/products/compute/amd-epyc-processors-come-to-google-and-to-google-cloud.

[110] Ari Levy, *AMD shares surge 16% after Google and Twitter say they're using the chipmaker's nw processor*, CNBC (Aug. 8, 2019), https://www.cnbc.com/2019/08/08/amd-shares-surge-14percent-after-google-and-twitter-sign-on-with-epyc-chips.html; Tom Warren, *Inside Microsoft's New Custom Surface Processors with AMD and Qualcomm*, The Verge (Oct. 2, 2019), https://www.theverge.com/2019/10/2/20888999/microsoft-surface-pro-x-laptop-3-custom-processor-qualcomm-amd.

[111] Andy Klein, *Petabytes on a Budget: 10 Years and Counting*, Backblaze (Sept. 24, 2019), https://www.backblaze.com/blog/petabytes-on-a-budget-10-years-and-counting/.

[112] *Cloud companies consider Intel rivals after the discovery of microchip security flaws*, CNBC (Jan. 10, 2018), https://www.cnbc.com/2018/01/10/cloud-companies-consider-intel-rivals-after-security-flaws-found.html.

[113] Matt Hanson, *Microsoft could ditch Intel for AMD with its Surface Laptop 3*, TechRadar (Sept. 16, 2019), https://www.techradar.com/news/microsoft-could-ditch-intel-for-amd-with-its-surface-laptop-3.

of international private technology firms—including some in China—Intel did not disclose the Meltdown and Spectre exploits to customers in the U.S. government, such as the National Security Agency or the Department of Homeland Security. Both of these agencies learned of the Meltdown and Spectre exploits the same way that the consuming public did—through news reports on or after January 3, 2018. As a result, the federal government could not assess the national security implications of the hardware exploits or take steps to defend federal computer systems against them during the months that researchers and private companies grappled with the crisis behind the scenes.

314. By not informing the U.S. government about the hardware exploits, Intel gave international interests an unimpeded advantage at improperly accessing U.S. systems. "It's really troubling and concerning that many if not all computers used by the government contain a processor vulnerability that could allow hostile nations to steal key data sets and information," New Hampshire Senator Maggie Hassan said during Congressional hearings. It is even more troubling that Intel knew about these exploits for nearly a year without notifying the federal government.

F. Intel's Interim Patches Have Impacted The Performance Of The CPUs And Still Leave The CPUs Vulnerable To Exploit

315. Plaintiffs and absent Class members have been harmed, injured, and damaged by, *inter alia,* Intel's acts, omissions, and practices in connection with its inherently and materially defective CPUs, which allow unauthorized users to steal confidential, valuable, and sensitive data. Furthermore, Intel's mitigation efforts to date have slashed the promised CPU performance and also failed to eliminate the ongoing security vulnerabilities of its CPUs. Having disregarded security considerations for years in connection with its design and development of Intel's CPUs (as described above), Intel has so fully integrated the Defects into its CPU-design that the only way to eliminate the security vulnerabilities is for Intel to redesign the defective portions of its CPUs.

316. Despite its knowledge of the Defects, Intel has been unable or unwilling to repair the Defects without substantial performance degradation, or offer Plaintiffs and Class members a non-defective Intel CPU or reimbursement for the cost of such defective CPUs and the consequential damages arising from the purchase and use of the defective CPUs.

317. Intel rushed initial fixes out, which resulted in many adverse consequences. Operating system patches were released, but these caused unacceptable data corruption and loss, and were quickly withdrawn. CPU microcode updates were released, but this resulted in disabled servers (causing many customers to steer clear of these risky updates). Intel, meanwhile, promised that future CPUs without the Defects would be "available soon"—which, of course, did nothing to address the millions and millions of vulnerable devices already in the market and in use.

318. Worse still, the available patches not only dramatically degrade the CPUs' performance, they do not even fix the Defects.

319. Indeed, the existing mitigations leave the door wide open for further exploits that take advantage of the same core Defects involving Intel's speculative execution, processor-caching and memory usage. Because the mitigations fail to address the underlying Defects and are only limited to the specifics of a particular exploit, further exploit variations that exploit the Defects will continue to emerge. In fact, since the Meltdown and Spectre exploits were publicly disclosed in January 2018, almost two-dozen *new* exploit variations have been identified, including the following:

INTEL CPU EXPLOIT	**CVE**	**ALIASES**
Foreshadow	2018-3615	L1 Terminal Fault-SGX

INTEL CPU EXPLOIT	**CVE**	**ALIASES**
Foreshadow-NG	2018-3620	L1 Terminal Fault-OS/ SMM
Foreshadow-NG	2018-3646	L1 Terminal Fault-VMM
Fallout	2018-2126	Store Buffer Data Sampling Microarchitectural Data Sampling
RIDL/ZombieLoad	2018-2127	Load Port Data Sampling Microarchitectural Data Sampling
RIDL/ZombieLoad	2018-2130	Fill Buffer Data Sampling Microarchitectural Data Sampling
SwapGS	2019-1125	
RIDL/ZombieLoad	2019-1091	Data Sampling Uncacheable Memory Microarchitectural Data Sampling
RIDL/ZombieLoad	2019-1135	Transactional Synchronization Extensions Asynchronous Abort Microarchitectural Data Sampling
Vector Register Sampling	2020-0548	

INTEL CPU EXPLOIT	CVE	ALIASES
CacheOut	2020-0549	L1D Eviction Sampling
Snoop-assisted L1D Sampling	2020-0550	
Load Value Injection	2020-0551	

320. Despite the continuous discovery of security vulnerabilities and the impact that corresponding mitigations have on performance, Intel continues to advertise and tout its processors' performance without regard to how future patches could affect processor performance and, thus, the central functionality of its CPUs.

321. The only way for Intel to put an end to this vicious security attack/mitigation patch cycle is for it to redesign its CPU microarchitecture and eliminate the Defects, and otherwise safeguard processor-caching and memory usage from side-channel attacks. Until then, Plaintiffs and absent Class members are left with the unappealing choice of spending money on a whole new computer that uses a rival CPU that does not contain the Defects, or continuing to use their Intel CPU-based computer which exposes them to substantial security risk and/or significant performance degradation (by as much as 40 percent) if the necessary mitigation patches are applied.

G. Intel's Failed Mitigation Attempts Have Resulted in Significant Negative Consequences

322. Even after the date that Intel claims it first learned of Meltdown and Spectre, it intentionally delayed disclosing the vulnerability for months, thereby increasing the exposure, risks,

and injury to Plaintiffs and Class members. Yet, even with such substantial lead-time, Intel was very slow to provide patches. The mitigations came nearly two months after the CPU vulnerabilities were first exposed publicly and nearly nine months after they were first reported to Intel.

323. Then, when it finally did deploy patches, albeit months too late, Intel's patches caused systems to reboot unexpectedly and led to data loss and corruption. Intel even advised consumers not to download its patches until better versions were deployed. Intel EVP Neil Shenoy stated that "[w]e recommend that OEMs, cloud service providers, system manufacturers, software vendors, and end users stop deployment of current versions on specific platforms as they may introduce higher than expected reboots and other unpredictable system behavior."[114] Intel then buried a warning in its latest financial results that its buggy firmware updates could lead to "data loss or corruption."[115]

324. Moreover, while it attempted to patch the exploits caused by its Defects in *certain* CPUs, Intel chose to ignore numerous systems affected by the Intel CPU Exploits and leave them vulnerable to exploit. CPU families that Intel will *not* patch include Bloomfield, Clarksfield, Gulftown, Harpertown Xeon C0, Harpertown Xeon E0, Jasper Forest, Penryn/QC, SoFIA 3GR, Wolfdale C0 and M0, Wolfdale E0 and R0, Wolfdale Xeon X0, Wolfdale Xeon E0, Yorkfield, and Yorkfield Xeon.[116]

---

[114] Joe Osborne, *Don't download Intel's latest Spectre and Meltdown patch, Intel Warns*, TechRadar (Jan. 22, 2018), https://www.techradar.com/news/dont-download-intels-latest-spectre-and-meltdown-patch-intel-warns.

[115] Tom Warren, *Microsoft issues emergency Windows update to disable Intel's buggy Spectre fixes*, The Verge (Jan. 29, 2018), https://www.theverge.com/2018/1/29/16944326/microsoft-spectre-processor-bug-emergency-windows-update-reboot-fix

[116] Liam Tung, *Intel: We now won't ever patch Spectre variant 2 flaw in these chips*, ZDNet.com (Apr. 4, 2018), https://www.zdnet.com/article/intel-we-now-wont-ever-patch-spectre-variant-2-flaw-in-these-chips/.

H. Intel's Interim Patches Have Come at a Significant Cost to the CPUs' Processing Speed and Performance

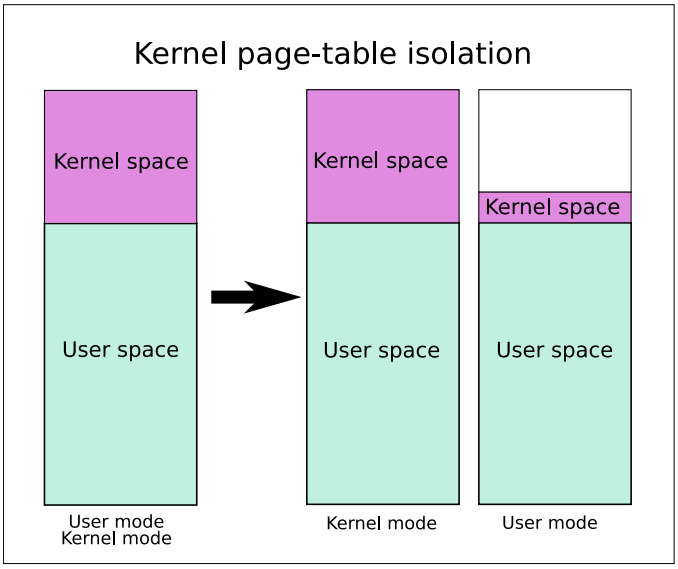
325. The Intel CPU Exploits, including the Meltdown, Foreshadow, RIDL, ZombieLoad, Fallout, L1 Data Eviction Sampling, Vector Register Sampling, L1D Snoop Sampling, Transactional Asynchronous Abort, Load Value Injection, and Spectre, which exploit the Defects in Intel's CPUs, are not just extraordinary issues of security, but also performance. Intel's mitigations cause substantial performance degradation, with some researchers, including those at Apple, claiming in excess of 40% loss in performance.[117]

326. The purported fixes carry performance costs, in part because the cache side-channel techniques exploit Intel's implementation of speculative execution, which as described above is a physical feature built into the Intel CPUs to speed up operations. Thus, safeguarding against attacks compromises marketed features and diminishes the speed and performance on which Intel distinguished its CPUs.

327. For example, to mitigate the Meltdown exploit, Intel recommends disabling key performance functionality through changes to operating system kernel code, including increased isolation of kernel memory from user-mode processes. This mitigation is often referred to as kernel page-table isolation ("KPTI," which is also referred to as KAISER). The protection is based on complete separation of kernel and user page tables. As a result, kernel and user programs exist in separate address spaces, effectively mitigating Meltdown, but not the other side-channel exploits. KPTI effectively mitigates Meltdown because user applications no longer can perform speculative

[117] *How to enable full mitigation for Microarchitectural Data Sampling (MDS) vulnerabilities*, Apple Support (June 7, 2019), https://support.apple.com/en-gb/HT210108.

memory accesses to kernel address space because the kernel is completely unmapped, as depicted below:



328. KPTI protection, though, comes at a substantial performance cost. The performance impact (often referred to as "overhead") of the KPTI patches alone was measured by Dave Hansen, a Linux kernel developer who works at Intel, to be anywhere from 5% to 30%, even with the PCID optimization[118]; for database engine PostgreSQL the impact on read-only tests on an Intel Skylake processor was 7% to 17% (or 16% to 23% without PCID),[119] while a full benchmark lost 13% to 19% (Coffee Lake vs. Broadwell-E).[120]

[118] Communication from Dave Hansen, *Patch 00/30 v.3 KAISER: unmap most of the kernel from userspace page tables*, LWN.net (Nov. 10, 2017), https://lwn.net/Articles/738997/.

[119] Communication from Andrews Freund, *headsup: Fix for intel hardware bug will lead to performance regressions*, PostgreSQL (Jan. 1, 2018), https://www.postgresql.org/message-id/20180102222354.qikjmf7dvnjgbkxe%40alap3.anarazel.de.

[120] Michael Larabel, *Initial Benchmarks Of The Performance Impact Resulting From Linux's x86 Security Changes*, Phoronix (Jan. 2, 2018), https://www.phoronix.com/scan.php?page=article&item=linux-415-x86pti&num=2.

329. KPTI patches, however, do not protect from any variation of the Foreshadow and Spectre exploits or when Meltdown is performed within the same address space, for example in the case of software modules protected with software fault isolation techniques.

330. To mitigate the Foreshadow exploits, Intel recommends implementing microcode and operating system updates and hypervisor changes (for cloud guests). Foreshadow mitigations enable a new feature called the ESXi Side-Channel-Aware Scheduler, also referred to as the ESXi SCA Scheduler. This scheduler will schedule the hypervisor and VMs on only one logical processor of an Intel Hyper-Threading-enabled core. This means the ESXi Side-Channel-Aware Scheduler will not make use of all the Hyper-Threading cores presented.

331. Like the KPTI patches, the Foreshadow mitigation techniques have a significant adverse impact on performance. For example, the performance impact observed in test environments for enterprise class workloads after implementing Foreshadow patches and enabling the ESXi Side-Channel-Aware Scheduler was as high as 32%.[121]

Application Workload / Guest OS	**Performance Degradation After Enabling Foreshadow Mitigations**
Database OLTP / Windows	32%
Database OLTP / Linux (with vSAN)	32%
Mixed Workload / Linux	25%
Java / Linux	22%
VDI / Windows	30%

332. Incredibly, aware that the performance impacts of mitigating this severe vulnerability created by its own flawed microarchitecture design decisions would be substantial for many

[121] *VMware Performance Impact Statement for 'L1 Terminal Fault-VNM' (L1tf-VMM) mitigations: CVE-2018-3646 (55767),* VMWare Knowledge Base (last updated Apr. 18, 2020), https://kb.vmware.com/s/article/55767#q=performance.

consumers, Intel attempted to impose a licensing restriction in order to prevent owners of its CPUs from using benchmark software to assess the extent of the performance overhead associated with patching their CPUs to prevent a Foreshadow exploit.[122]

333. To mitigate the MDS exploits (including MDSUM, MFBDS, MLPDS, MSBDS, TAA, L1DES and VRS exploits), Intel recommends fixes to operating systems, virtualization mechanisms, web browsers, and microcode patches that flush intermediate processor buffers when switching to a lower privileged level.

334. Intel has also recommended that users disable Hyper-Threading or employ a group scheduler. Intel describes Hyper-Threading as a technique for improving processor efficiency: "Simultaneous multithreading (SMT) is a technique for improving the overall efficiency of superscalar CPUs with hardware multithreading. SMT permits multiple independent threads of execution to better utilize the resources provided by modern processor architectures. Intel® Hyper-Threading technology (Intel® HT) is Intel's implementation of SMT." Intel has claimed that Hyper-Threading results in performance improvements of close to 30%.[123]

335. To mitigate TAA exploits, Intel recommends disabling transactional memory extensions, or applying all the mitigations used to mitigate RIDL, ZombieLoad, Fallout, and Vector Register Sampling exploits. Disabling transactional memory exploits, though, can result in significant performance degradation for workloads that use transactional memory, especially when Hyper-Threading is disabled. It is well known that transactional memory makes it simpler for programmers to write high performance parallel code. A paper published by Intel researchers

[122] *Software License for Intel Memory Latency Checker (Intel MCL),* Intel https://software.intel.com/en-us/protected-download/739797/493768 (last visited May 5, 2020).

indicated that "on a set of real-world, high performance computing workloads, Intel TSX provides 1.41x average speedup over lock- and atomics-based implementations… [and] 1.31x bandwidth improvement on a set of network intensive applications."[124]

336. The mitigations to protect against the MDS exploits result in an adverse impact of 8% to 10% in performance without disabling Hyper-Threading.[125] Apple, though, has warned that its own tests have shown as much as a 40% reduction in performance when its Mac computers handle certain computing-intensive workloads.[126]

337. Despite Intel's mitigations (and their resulting impact on CPU performance), L1D Eviction Sampling/CacheOUT, was reported in processors that had Intel's microcode patches to protect against RIDL/ZombieLoad exploits. According to RedHat (IBM), Intel's fix did not properly clear the fill buffers during its mitigation (they left out some "corner cases"), and the Cacheout exploit exposed this issue. This is another instance of how Intel's piecemeal approach to mitigation and failure to fix the underlying Defects leaves the door open for more exploits.[127]

338. Similarly, Vector Register Sampling was reported in processors that had Intel's microcode patches to protect against the Fallout exploit. According to RedHat (IBM), Intel's fix did not take into account the fact that program instructions can complete after Intel's patches cleared

---

[124] R. M. Yoo, et al. *Performance Evaluation of Intel Transactional Synchronization Extensions for High-Performance Computing*, (2013), http://pages.cs.wisc.edu/~rajwar/papers/SC13_TSX.pdf.

[125] Michael Larabel, *Benchmarking AMD FX vs. Intel Sandy/Ivy Bridge CPUs Following Spectre, Meltdown, L1TF, Zombieload*, Phoronix (May 24, 2019), https://www.phoronix.com/scan.php?page=article&item=sandy-fx-zombieload&num=1.

[126] *Intel Zombieload bug fix to slow data centre computers*, BBCNews (May 15, 2019), https://www.bbc.com/news/technology-48278400.

[127] *CVE-2020-0549*, Red Hat (Jan. 27, 2020), https://access.redhat.com/security/cve/cve-2020-0549.

out the buffers. Moreover, Intel has yet to release a microcode patch or other mitigation to protect against Vector Register Sampling.

339. To mitigate a class of vulnerabilities known as Snoop Assisted L1 Sampling, Intel recommends flushing the L1 Data cache before executing potentially unauthorized applications.

340. Mitigations against the Load Value Injection exploit are particularly catastrophic for Intel SGX. Essentially, any instruction that involves memory while in SGX mode will need to be executed non-speculatively. Depending on the execution properties of the Intel SGX enclave workload (for example, CPU-bound vs. I/O-bound, cache locality, etc.), the performance impact of mitigation will vary depending on workload but can be significant.

341. Notably, one of the features that enables SGX exploits using Load Value Injection is Intel's fix against the Meltdown exploit in hardware (in processors after the Whiskey Lake generation). These processors produce a value 0x00 for a load that "faults" (instead of returning the value in the cache as is the case in processors without the hardware mitigations). The value 0x00 can be considered a valid memory address in SGX mode, and an unauthorized user can map arbitrary pages at this address to leak information through loads that depend on the faulting load.

342. The Load Value Injection mitigation techniques have a significant adverse impact on performance. For example, the performance impact observed in test environments on Intel's Kaby Lake processors resulting in adverse performance impact of 22%.[128] Mitigations proposed by a

[128] Michael Larabel, *The Brutal Performance Impact for Mitigating the LVI Vulnerability*, Phoronix (Mar. 12, 2020), https://www.phoronix.com/scan.php?page=article&item=lvi-attack-perf&num=1.

Google engineer to protect against the Load Value Injection exploit and other side-channel exploits saw just 7% the original performance in one of her tests.[129]

343. To mitigate the Spectre exploits, Intel also recommends implementing separate microcode updates and retpoline compiler changes.

344. In total, there are at least seven layers of performance overhead related to Intel's mitigations for the Intel CPU Exploits. They include:

- Guest kernel KPTI patches
- Intel microcode updates
- Cloud provider hypervisor changes (for cloud guests)
- Retpoline compiler changes
- Software to flush the L1 data cache
- Compiler de-optimization for SGX code
- Disabling Hyper-Threading

345. Intel's mitigations affect real-world application benchmarks and cause a massive drain on CPU performance.[130] Exactly how much the system is impacted depends on the characteristics of the application being tested. As Brendan Gregg, a senior performance architect at Netflix, explained, applications with higher system call (or syscall) rates, such as proxies and

[129] *[x86][seses] Introduce SESES pass for LVI*, Phabricator, https://reviews.llvm.org/D75939 (as published Mar. 10, 2020) (last visited May 28, 2020); s*ee also* Michael Larabel, *Google Engineer Shows 'SESES' for Mitigating LVI + Side-Channel Attacks – Cod Runs ~ 7% Original Speed*, Phoronix (Mar. 21, 2020), https://www.phoronix.com/scan.php?page=news_item&px=LLVM-SESES-Mitigating-LVI-More.

[130] Brendan Gregg, *KPTI/KAISER Meltdown Initial Performance Regressions*, Brendan Gregg's Blog (Feb. 9, 2018), http://www.brendangregg.com/blog/2018-02-09/kpti-kaiser-meltdown-performance.html.

databases that do lots of I/O (input/output), will suffer the largest losses. The impact also rises with higher context switch and page fault rates.[131] The severity of the impact will also depend on the CPU overcommit ratio on a given host and the host utilization.[132]

346. Nevertheless, performance testing has confirmed that all Plaintiffs and members of the Class suffer material performance regressions as a direct consequence of installing Intel's mitigations.

347. Based on side-by-side comparisons between systems built from different generations of Intel CPUs, the patches issued to mitigate the Defects inherent in Intel's defective CPUs (which, for many, disable marketed functionality and features of the CPUs) reduce the performance of a given Intel CPU model to that of a CPU model of several generations prior.

I. Performance Matters

348. Computer processing performance is fundamental to basic computer functionality.

349. Performance significantly impacts user experience. Users *really* care about speed in interactive environments. Responsiveness is a key feature that consumers expect from their computer system. That is because responsiveness is a basic user interface design rule that's dictated by human needs, not by individual technologies.

350. Responsiveness matters for two reasons:

---

[131] Brendan Gregg, *KPTI/KAISER Meltdown Initial Performance Regressions*, Brendan Gregg's Blog (Feb. 9, 2018), http://www.brendangregg.com/blog/2018-02-09/kpti-kaiser-meltdown-performance.html.

[132] *VMware Performance Impact Statement for 'L1 Terminal Fault-VNM' (L1tf-VMM) mitigations: CVE-2018-3646 (55767)*, VMWare Knowledge Base (last updated Apr. 18, 2020), https://kb.vmware.com/s/article/55767#q=performance.

- Human limitations, especially in the areas of memory and attention. Users simply do not perform as well if they have to wait and suffer the inevitable decay of information stored in short-term memory.
- Human aspirations. Users like to feel in control of their destiny rather than subjugated to a computer's whims.[133]

351. A faster user experience beats a glamorous one, for the simple reason that people engage more when they can move freely and focus on the content instead of on their endless wait.

352. Users who run more than one application at a time (i.e., multitasking) depend on tasks being managed in such a way as to create an illusion that each task has a dedicated CPU all to itself, which allows users to have several applications open and working at the same time without interruption:

[133] Jakob Nielson, *Website Response Times*, Nielsen Norman Group (June 20, 2010), https://www.nngroup.com/articles/website-response-times/.

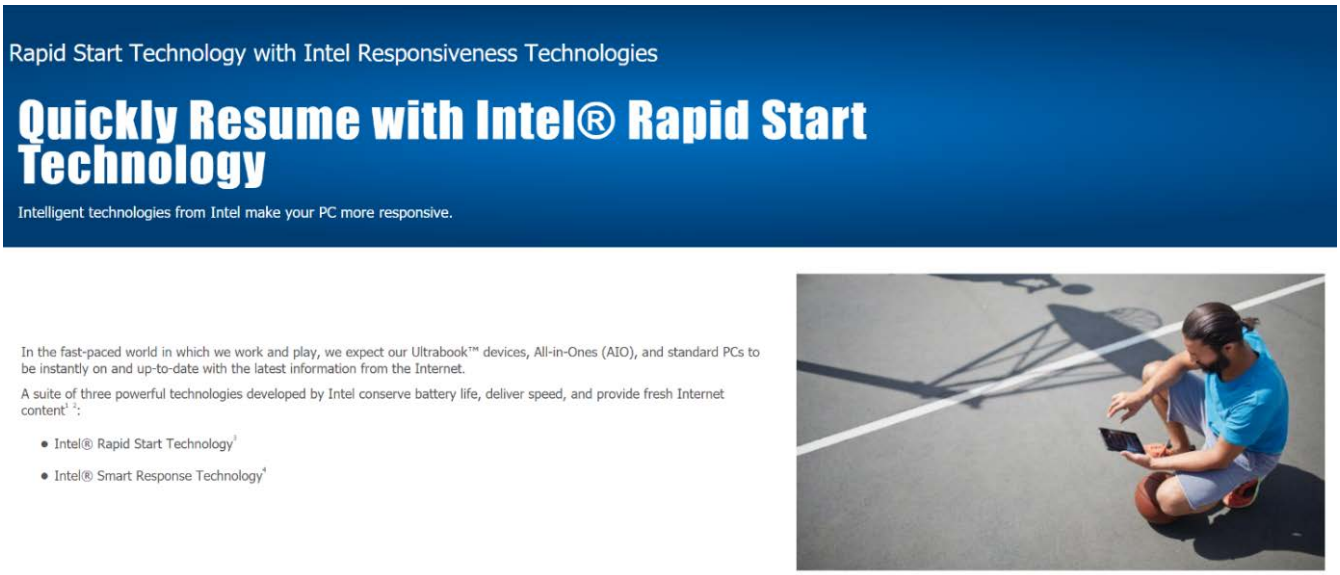
353. When talking about responsiveness to performance requests, milliseconds matter. Even delays of a fraction of a second are perceived by users, and disconnect the user from their experience, and their action and reaction.[134]

354. Studies show that responsiveness affects users' stress level and their own performance. Responsiveness has been shown to be one of the strongest stressors in human-computer interaction.[135]

355. Recognizing the role that responsiveness plays in user experience, Intel has nurtured a computer culture focused on processing power and performance. It advertises the responsiveness advantages of the products it brings to the market. Notably, responsiveness has been one of the key features that Intel has emphasized over the years in presentations and marketing materials, as can be seen from the following promotional example:

[134] M. Kearny, A. Osmani, K. Basques, J. Miller, *Measure Performance with the RAIL Model*, Google Web Fundamentals, https://developers.google.com/web/fundamentals/performance/rail (last visited May 5, 2020).

[135] Noah Stupak, *Time delays and system response times in human-computer interaction*, Rochester Institute of Technology RIT Scholar Works (Sept. 10, 2009), https://scholarworks.rit.edu/cgi/viewcontent.cgi?article=2374&context=theses.

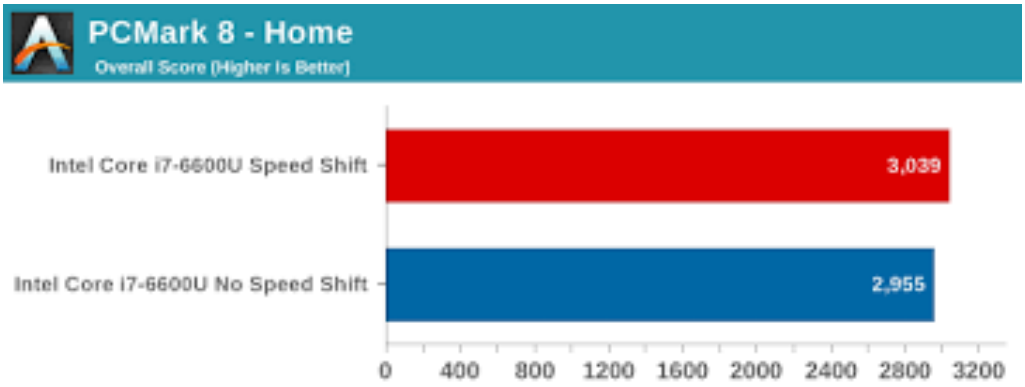


https://www.intel.com/content/www/us/en/architecture-and-technology/responsiveness-technologies.html.

https://www.intel.com/content/www/us/en/products/docs/devices-systems/laptops/laptop-innovation-program.html?utm_source=facebook&utm_medium=social&CID=iosm|&linkId=100000010719482.

356. Indeed, Intel invested many millions of dollars in research, development, manufacturing, and marketing of its Speed Shift technology, which Intel touted as delivering

dramatically quicker responsiveness with single-threaded, transient (short duration) workloads, such as web browsing, by allowing the processor to more quickly select its best operating frequency and voltage for optimal performance and power efficiency. Previously, it took about 20-30 milliseconds for a processor to inform the operating system that something has happened (the workload has gone up, the system is getting too hot, etc.) and for the operating system to then respond (increase the frequency to handle the workload, reduce the frequency to reduce power draw). Intel's Speed Shift technology reduced the time that a CPU typically takes to 1ms (i.e., a 19ms gain)[136]:



https://wccftech.com/intel-introduces-speed-shift-technology/.

357. Like Intel, computer makers feature processing power as the heart of their advertising. Hewlett Packard's website affirms that "[c]omputer processor speed [] is one of the most important elements to consider when comparing computers." [137] On May 21, 2019, Apple introduced what was deemed "the fastest Mac notebook ever" due to its new "faster 8th- and 9th-

[136] Usman Pirzada, *Intel Introduces Speed Shift Technology for Skylake 6th Generation Processors – Will Be Landing This Month Via A Windows 10 Update*, WCCFTech (Nov. 10, 2015), https://wccftech.com/intel-introduces-speed-shift-technology/.

[137] *See* Sophie Sirois, *What is Processor Speed and Why Does It Matter*, HP Tech Takes (Dec. 18, 2018), https://store.hp.com/us/en/tech-takes/what-is-processor-speed.

generation Intel Core processors."[138] Dell also points to the functional importance of a processor where it assists potential customers in understanding processors by stating, "The processor is the engine behind your computer processing critical information and instructions. The speed at which your system runs programs, loads pages and downloads files depends … on the processor."[139]

358. All of Intel's marketed performance gains (and then some), though, are lost by installing Intel's mitigations for the Intel CPU Exploits. Because the mitigations essentially downgrade the processor back to performance levels of a prior CPU generation, a consumer is left with a computer that has substantially different CPU specifications than originally purchased.

J. Intel's Performance Degradation in Context

359. Every 12 to 18 months, Intel releases a new processor generation, and within each generation Intel's core processors are divided into tiers (e.g., Core i3 [entry-level], Core i5 [mainstream], Core i7 [high-end], and Core i9 [highest-end]), with several models in each tier.

360. Intel has touted and relied upon single-digit performance gains to market, advertise, and sell its new generation of processors as well as differentiate its processors within tiers. Thus, these performance advancements are material to Intel and consumers because Intel has used them to justify its premium price for newly released CPUs and between processors within the same generation tiers, as well as the millions of dollars invested in their research, development, manufacturing, and marketing.

---

[138] *Apple introduces first 8-core MacBook Pro, the fastest Mac notebook ever*, Apple (May 21, 2019), https://www.apple.com/newsroom/2019/05/apple-introduces-first-8-core-macbook-pro-the-fastest-mac-notebook-ever/.

[139] *Steps to choose an Intel Processor/CPU for your PC*, Dell, https://www.dell.com/learn/us/en/98/campaigns/how-to-choose-an-intel-processor-cpu (last visited May 2, 2020).

361. Each new CPU generation is generally more expensive than the CPUs it has replaced. For example, Intel sold its 6th generation Core processors, christened Skylake, at a higher price than it sold the previous generation Core processors, which it had christened Broadwell.

362. In general, the higher the tier within each generation the more expensive the CPU. For example, Intel Core i7 processors are sold at a higher price than its Core i5 processors, which, in turn, are sold at a higher price than Intel Core i3 processors.

363. For example, Intel promised that Haswell processors, its 4th generation Core processors, would achieve 5% to 15% performance gains over Ivy Bridge, which was its 3rd generation Core processors. Performance testing comparing Haswell processors to Ivy Bridge processors revealed performance gains of 1% to 19%, with an average improvement of 8.3%. Compared to Sandy Bridge, Intel's 2nd generation Core processors, Haswell processor yielded a performance improvement of 7% to 26%, with an average performance advantage of 17%.[140]

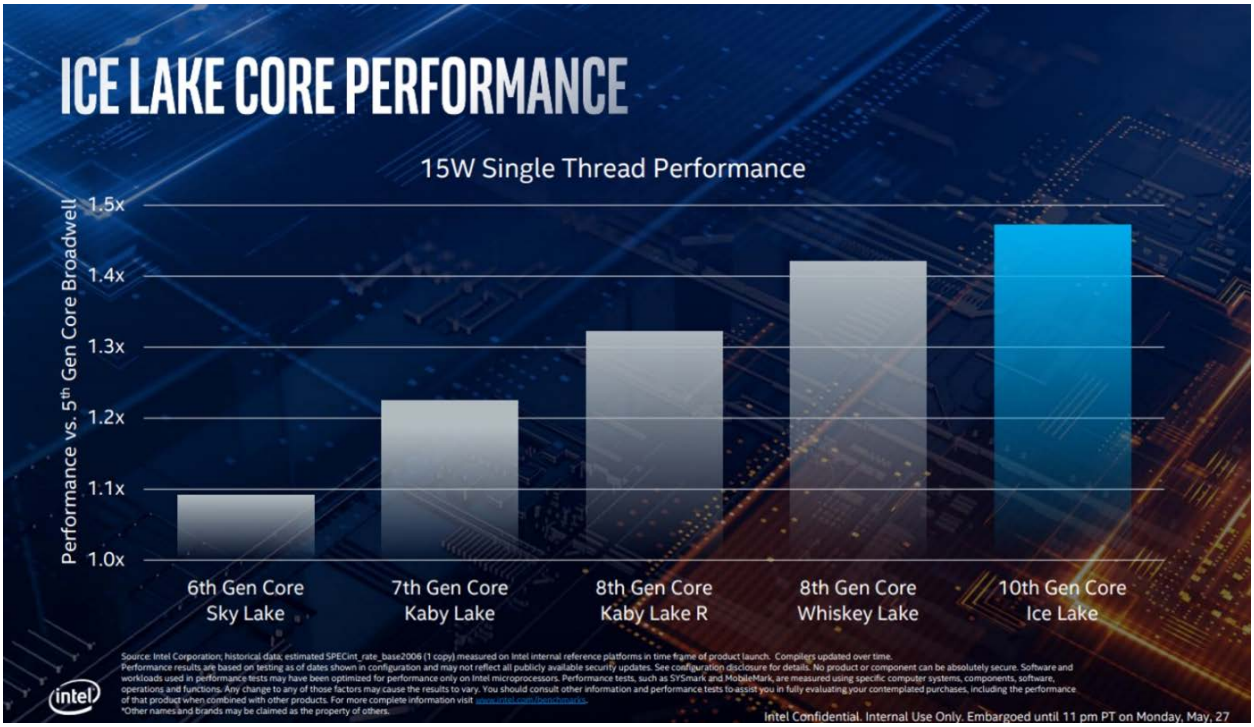
364. Performance testing comparing Intel's 5th generation Core processors, Broadwell processors, to its prior 4th generation Core processors, Haswell processors, shows the two generations' performance to be "very close." Broadwell processors performed better than Haswell processors by approximately 5% to 10% on a given task when the CPU models were exactly the same.[141]

365. Indeed, Intel's own marketing material touted performance benefits of 5% to 11% when upgrading from one generation of CPU to the next—considerably less than the performance

[140]Anand Lal Shimpi, *The Haswell Review: Intel Core i7-4770K & i5-4670K Tested*, AnandTech (June 1, 2013), https://www.anandtech.com/show/7003/the-haswell-review-intel-core-i74770k-i54560k-tested/6.

[141] Gordon Mah Ung, *The truth about Intel's Broadwell vs. Haswell CPU*, PCWorld (July 6, 2015), https://www.pcworld.com/article/2940489/the-truth-about-intels-broadwell-vs-haswell-cpu.html.

decline resulting from the Intel CPU Exploits' mitigations. In the below figure, adjacent bars represent the relative performance of successive generations of Intel processors:



366. In view of the foregoing—by standards Intel has acknowledged are material to purchasers and that it uses to price its CPUs—the performance impacts caused by installation of its mitigations to address the Defects in its CPUs are material to users.

K. The Only True "Fix" for the Security Vulnerabilities Inherent in Intel's Defective CPUs Is a New CPU

367. Researchers have confirmed that all of the Intel CPU Exploits but for Spectre are unique to Intel CPUs, and that a proper implementation of speculative execution would have prevented these exploits.

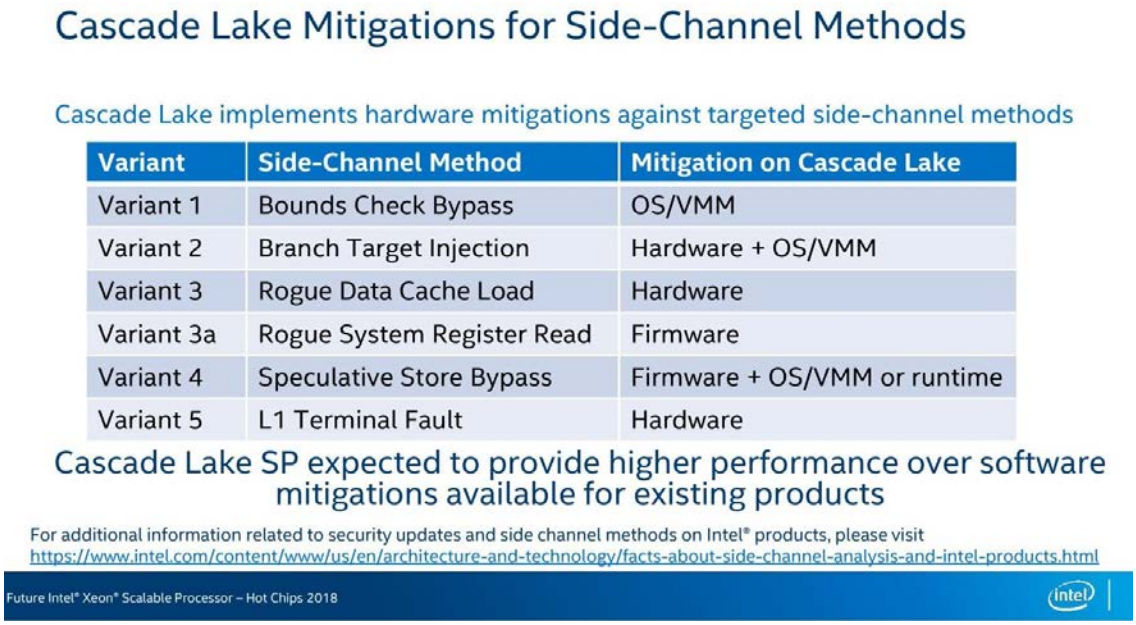
368. Intel's mitigations to date only attempt to address the specifics of each exploit (as opposed to correcting the underlying CPU Defects) so its CPUs remain vulnerable to new exploit variations. Moreover, although Intel has deployed patches to mitigate Intel CPU Exploits, the

mitigations are only band-aids. In fact, the real fix, according to researchers and even Intel, is remedying its defective CPU design.[142]

369. Thus, Intel's only *true* fix is a CPU microarchitecture that safeguards processor-caching and memory usage from side-channel exploit.

370. To this end, Intel's former CEO Brian Krzanich announced that Intel expected to ship a CPU with hardware fixes for its defective design by the end of 2018.[143]

371. Intel released Cascade Lake in 2018. Intel's Cascade Lake purported to fix for Meltdown, Foreshadow, and Spectre, as follows:



Cascade Lake Mitigations for Side-Channel Methods

Cascade Lake implements hardware mitigations against targeted side-channel methods

Variant	Side-Channel Method	Mitigation on Cascade Lake
Variant 1	Bounds Check Bypass	OS/VMM
Variant 2	Branch Target Injection	Hardware + OS/VMM
Variant 3	Rogue Data Cache Load	Hardware
Variant 3a	Rogue System Register Read	Firmware
Variant 4	Speculative Store Bypass	Firmware + OS/VMM or runtime
Variant 5	L1 Terminal Fault	Hardware

Cascade Lake SP expected to provide higher performance over software mitigations available for existing products

For additional information related to security updates and side channel methods on Intel® products, please visit https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html

Future Intel® Xeon® Scalable Processor – Hot Chips 2018

intel

[142] *VMware Performance Impact Statement for 'L1 Terminal Fault-VNM' (L1tf-VMM) mitigations: CVE-2018-3646 (55767)*, VMWare Knowledge Base (last updated Apr. 18, 2020), https://kb.vmware.com/s/article/55767#q=performance.

[143] Ian Cutress, *Intel at Hot Chips 2018: Showing the Ankle of Cascade Lake*, AnandTech (Aug. 19, 2018), https://www.anandtech.com/show/13239/intel-at-hot-chips-2018-showing-the-ankle-of-cascade-lake.

372. As originally planned, the Cooper Lake line was going to be dropped near the end of 2019 before being replaced by a 2020 Ice Lake. Intel mostly cancelled Cooper Lake, and the limited segments to be released have been delayed to sometime in 2020.

CLASS ACTION ALLEGATIONS

373. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of a Class ("the National Class") defined as follows:

> All persons or entities that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in the United States and its territories since January 1, 2006 to the present.

374. In addition to the Nationwide Class, and pursuant to Federal Rule of Civil Procedure Rule 23(c)(5) and/or the respective state statute(s), Plaintiffs seek to represent all members of the following Subclass of the National Class, as well as any subclasses or issue classes as Plaintiffs may propose and/or this Court may designate at the time of class certification, including but not limited to claims under the consumer protection and unfair and deceptive trade practices statutes of each of the jurisdictions below in each of those jurisdictions:

> All persons or entities that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in the United States and its territories since January 1, 2006 to the present within Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South

Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, and Wisconsin.

375. Plaintiffs reserve their rights before the Court determines whether certification is appropriate to redefine the proposed class, or to propose subclasses, if necessary or alternatively, including but not limited to state subclasses (*i.e.*, the Alabama Subclass, the Washington Subclass, etc.) and/or entity subclasses.

376. Collectively, unless otherwise so stated, the above-defined classes and subclasses are referred to herein as the "Class."

377. Excluded from the Class are: (1) Intel, its subsidiaries, affiliates, officers, directors, employees, agents, and contractors; (2) persons or entities that have settled with and validly released Intel from separate, non-class legal actions based on the conduct alleged herein; and (3) the Court and its personnel and relatives.

378. Plaintiffs reserve their right to amend the Class definitions if discovery and further investigation reveal that the Class collectively or any individual class or subclass should be expanded or narrowed, divided into additional subclasses pursuant to Rule 23(c)(5), or modified in any other way.

379. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** Class members are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. Plaintiffs are informed and believe—based upon the publicly-available information discussed herein—that there are millions of Class members throughout the country, making joinder impracticable.

380. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).** Intel has acted with respect to Plaintiffs and the other members of the proposed Class

in a manner generally applicable to each of them. There are numerous questions of law and fact common to Plaintiffs and Class members that predominate over any question affecting only individual Class members. The answers to these common questions will advance the adjudication or resolution of the litigation as to all Class members. The questions of law and fact common to the Class that predominate over the questions that may affect individual Class members include the following:

a. Whether Intel engaged in the conduct alleged herein;

b. Whether Intel designed, manufactured, advertised, promoted, and sold CPUs that it knew were defective, and withheld material information regarding the defective nature from consumers or purposely misrepresented the CPUs to consumers;

c. Whether Intel designed or manufactured the chips in such a way that made them susceptible to security exploits, allowing for side-channel exploits;

d. Whether and to what extent Intel disclosed the effect of the Defects on device security and, ultimately, performance;

e. Whether Intel induced Plaintiffs and the other Class members to purchase devices containing its CPUs that were advertised as secure yet fast and, if so, to what extent it profited from its inducements;

f. Whether Plaintiffs and absent Class members received the benefit of their bargain in purchasing the Intel CPUs;

g. Whether Plaintiffs and absent Class members overpaid for the Intel CPUs in light of the diminished processor performance resulting from installation of the various mitigations for the Defects;

h. Whether Intel was under a duty to disclose the true nature of the Intel CPUs to

consumers;

i. Whether the true nature of the Intel CPUs constitute material facts that reasonable consumers would have considered in deciding whether to purchase the Intel CPUs or computers containing them;

j. Whether Intel concealed material facts from Plaintiffs and absent Class members;

k. Whether Intel's conduct violated consumer protection statutes, false advertising laws, warranty laws, and common laws asserted herein;

l. Whether Plaintiffs and absent Class members are entitled to equitable relief, including, but not limited to, restitution, declaratory and injunctive relief.

f. Whether Intel has been unjustly enriched as a result of its improper conduct, such that it would be inequitable for Intel to retain the benefits conferred upon it by Plaintiffs and the other Class members;

g. The aggregate compensatory or consequential damages that should be awarded to Plaintiffs and absent Class members; and

h. Whether Intel's conduct in actively suppressing knowledge of the Defects rises to a level of egregiousness that warrants an award of punitive damages.

381. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of absent Class members' claims because Plaintiffs and Class members were subjected to the same allegedly unlawful conduct and damaged in the same way. Plaintiffs' claims are based on the same legal theories as the claims of all other members of each of their respective class. Moreover, Plaintiffs seek the same forms of relief for themselves as they do on behalf of absent Class members.

382. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate class representatives because they assert claims that are typical of those of absent Class members, giving them every incentive to vigorously pursue those claims and protect absent members' interests. Plaintiffs' interests do not conflict with the interests of the other Class members who they seek to represent, they are represented by counsel seasoned in consumer class action litigation (whom the Court has already appointed on an interim basis pursuant to Rule 23(g) to lead the litigation), and Plaintiffs intend to prosecute this action vigorously. Absent Class members' interests will be adequately protected by Plaintiffs and their counsel.

383. **Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2).** Intel has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate. Injunctive relief is particularly necessary in this case because: (1) Plaintiffs and absent Class members desire to purchase products with the same qualities and attributes as Intel advertised the Intel CPUs to have; (2) if Intel actually manufactured Intel CPUs with the performance and security advertised, Plaintiffs would purchase those Intel CPUs; (3) Plaintiffs do not, however, have the ability to determine whether Intel's representations concerning the Intel CPUs will be truthful if they purchase Intel CPUs or computers containing Intel CPUs in the future. Indeed, Plaintiffs, and absent Class members may in the future want to purchase Intel CPUs or computers containing Intel CPUs, but they expect that Intel will continue to misrepresent or conceal defects in those processors.

384. **Superiority: Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and Class members are relatively small

compared to the burden and expense that would be required to individually litigate their claims against Intel, so it would be impracticable for Class members to individually seek redress for Intel's wrongful conduct. Even if Class members could afford to pursue individual litigation, the court system could not handle a deluge of individual suits. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. The benefits of proceeding on a class-wide basis, including providing injured persons or entities with a method for obtaining redress for claims that might not be practicable to pursue on an individual basis substantially outweigh any potential difficulties in managing this litigation on a class basis.

TOLLING OF APPLICABLE LIMITATIONS PERIODS

385. **Discovery Rule Tolling.** Neither Plaintiffs nor absent Class members could have discovered, through the exercise of reasonable diligence, that their Intel CPUs had serious security Defects within the time period of any applicable statutes of limitation. As described herein, substantial technical expertise is required to uncover and comprehend the existence of the Defects alleged herein, and the ordinary reasonable consumer could not—with reasonable diligence—discover that their CPUs were affected by the Defects and were consequently vulnerable to side-channel exploits until experts started publicly voicing their research and concerns.

386. **Fraudulent Concealment Tolling.** Throughout the time period relevant to this action, Intel concealed from and failed to disclose to Plaintiffs and absent Class members vital information concerning the Intel CPUs. Indeed, Intel kept Plaintiffs and absent Class members ignorant of vital information essential to the pursuit of their claims. As a result, neither Plaintiffs

nor absent Class members could have discovered the Defects and security flaws, even upon reasonable exercise of diligence.

387. Despite its knowledge of the above, Intel failed to disclose and concealed, and continues to conceal, critical information from Plaintiffs and absent Class members, even though, at any point in time, it could have communicated material information through individual correspondence, media releases, or other means. Although Intel has finally acknowledged the security Defects in its chips, it waited years to do so, and has continued to conceal the true risks that one faces in using its CPUs.

388. Plaintiffs and absent Class members relied on Intel to disclose any defects in their CPUs, because those defects were hidden and not discoverable through reasonable efforts by Plaintiffs and absent Class members.

389. Thus, the running of all applicable statutes of limitation has been suspended with respect to any claims that Plaintiffs and absent Class members have sustained as a result of the Defects, by virtue of the fraudulent concealment doctrine.

390. **Estoppel.** Intel was under a continuous duty to disclose to Plaintiffs and the other Class members the true nature, quality, and character of its CPUs. Intel, however, concealed the true nature, quality, and character of the CPUs, as described herein. Based upon the foregoing, Intel is estopped from relying on any statutes of limitations in defense of this action.

CLAIMS ALLEGED

NATIONWIDE COUNT I

FRAUD BY CONCEALMENT AND OMISSION

COMMON LAW CLAIM

391. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

392. Plaintiffs bring this cause of action for themselves and on behalf of the Class. In the alternative, Plaintiffs bring this claim on behalf of each state subclass under the law of each state in which Class or subclass members purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU.[144]

393. At all relevant times, Intel was engaged in the business of designing, manufacturing, distributing, and selling CPUs.

394. Intel, acting through its representatives or agents, delivered CPUs to distributors, computer manufacturers, and various other distribution channels.

395. To increase sales and maintain its market power in light of increasing sales from other market competitors such as AMD, Intel marketed and advertised to consumers that its CPUs were secure, powerful, and fast performing.

396. Intel willfully, falsely, and knowingly concealed and omitted material facts regarding the quality and character of the CPUs, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that

[144] Accordingly, "Class members" or "absent Class members" also refers to the absent members of any Subclass.

necessary mitigations to address the Defects would result in significant CPU performance degradation, and that ,in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

397. Plaintiffs and Class members could not have discovered the omitted material facts on their own because Intel had exclusive or superior knowledge regarding the proprietary design of its CPUs, including the manner in which it implemented speculative and out-of-order execution. Only in January 2018 did it become public, after Plaintiffs and absent Class members had purchased products with Intel CPUs, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, and that mitigations to address the Defects would result in significant CPU performance degradation.

398. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

399. Plaintiffs and absent Class members sustained economic injury due to the purchase of the CPUs and products containing those CPUs. Specifically, they did not receive the benefit of

their bargain, namely, a CPU with the advertised security and performance. Instead, Plaintiffs and absent Class members received CPUs with the Defects and after patching their machines with the recommended mitigations, the CPUs suffered from significant performance degradation. Plaintiffs and absent Class members had the reasonable expectation that the CPUs would perform as advertised and represented. They are entitled to recover full or partial refunds for the CPUs, or they are entitled to damages for loss of the benefit of the bargain or the diminished value of their CPUs, amounts to be determined at trial.

400. Intel's acts were done wantonly, maliciously, oppressively, deliberately, and with intent to defraud; in reckless disregard of the rights of Plaintiffs and absent Class members; and to enrich itself. Intel's misconduct warrants an assessment of punitive damages in an amount sufficient to deter such conduct in the future especially given the threat environment created by consumers' constant need for connectivity. Punitive damages, if assessed, shall be determined according to proof at trial that Intel's acts were done maliciously, oppressively, deliberately, and with intent to defraud, and in reckless disregard of Plaintiffs' and absent Class members' rights, and in part to enrich itself at the expense of consumers. Intel's acts were done to gain commercial advantage over competitors, and to drive consumers away from consideration of competitors' CPUs. Intel's conduct warrants an assessment of punitive damages in an amount sufficient to deter such conduct in the future.

NATIONWIDE COUNT II

VIOLATIONS OF THE CONSUMERS LEGAL REMEDIES ACT

Cal. Civ. Code § 1750 *et seq.*

401. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

402. Those Plaintiffs that are not Enterprise Entities bring this cause of action for themselves and on behalf of the similarly situated members of the Class and/or on behalf similarly situated members of the California Subclass.

403. The Consumers Legal Remedies Act, Cal. Civ. Code § 1750 *et seq.* ("CLRA"), is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

404. In accordance with the liberal application and construction of the CLRA, application of the CLRA to all Class members is appropriate, given that Intel's conduct as described herein originated from California, the Intel CPUs were designed in California, and Intel's marketing materials were developed in California.

405. Intel is a "person" as defined by Cal. Civil Code §§ 1761(c) and 1770 and has provided "goods" as defined by Civil Code §§ 1761(a) and 1770.

406. Plaintiffs and Class members are "consumers" as defined by Cal. Civil Code §§ 1761(d) and 1770 and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

407. Intel's acts and practices were intended to and did result in the sales of goods and services to Plaintiffs and Class members in violation of Cal. Civil Code § 1770, including:

408. Representing that goods or services have characteristics that they do not have;

409. Representing that goods or services are of a particular standard, quality, or grade when they were not;

410. Advertising goods or services with intent not to sell them as advertised; and

411. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

412. Intel's misrepresentations and omissions were material because they were likely to deceive reasonable consumers.

413. Intel has engaged in a decades-long advertising campaign to market its CPUs as having built-in security and fast performance, using all mediums of advertising.

414. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

415. Plaintiffs and absent Class members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered with reasonable diligence.

416. As a direct and proximate result of Intel's violations of California Civil Code § 1770, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs or machines containing them, and increased time

and expense in installing patches to help resolve some of the CPU security issues (at the expense of speed and at risk of crashing their machines), and otherwise purchasing CPUs that were not defective.

417. Intel has already received notice of Class members' intent to seek damages in compliance with California Civil Code § 1782(a) and has failed to cure. Intel also received a supplemental notice pursuant to California Civil Code § 1782 concerning its wrongful conduct as alleged herein by Plaintiffs and absent Class members. Any further notice would be futile because Intel has yet to offer relief to the Class, despite being on notice of its unfair, deceptive, and fraudulent conduct.

418. As a result of Intel's conduct as alleged herein, Plaintiffs and Class members have been damaged.

419. Plaintiffs, on behalf of themselves and all Class members, seek an order enjoining the acts and practices alleged unlawful herein, and also seek damages for Intel's unlawful acts in an amount to be proven at trial.

NATIONWIDE COUNT III

VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW

Cal. Bus. & Prof. Code § 17200 *et seq.*

420. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

421. Plaintiffs bring this cause of action for themselves and on behalf of the Class and/or on behalf of the California Subclass.

422. In accordance with the liberal application and construction of the Unfair Competition Law ("UCL"), application of the UCL to all Class members is appropriate, given that Intel's

headquarters is in Santa Clara, California; Intel's conduct as described herein originated from California; Intel's marketing campaign was devised in California; and the decisions regarding the design of their CPU's emanated from California.

423. Intel is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

424. Intel violated Cal. Bus. & Prof. Code § 17200 *et seq.* by engaging in unlawful, unfair, and deceptive business acts and practices.

425. Intel has engaged in "unfair" business acts or practices by:

426. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with the Defects, which go toward their central functionality, resulting in security risks, compromising confidential information, and—if patched—significantly degrading CPU performance thereby, again, impacting their central functionality, so that consumers did not receive the benefit of their bargain;

427. Implementing speculative execution in a defective manner and thereby sacrificing security for speed for the purpose of increasing profits, despite knowing about the attendant security vulnerabilities;

428. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, therefore, putting profits over the safety of consumer data;

429. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

430. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

431. Making affirmative public representations about the speed of Intel CPUs while knowing that, in order for those CPUs to offer security for consumers' data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

432. Concealing and/or failing to disclose material facts, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

433. Intel's practices constitute unfair business practices in violation of the UCL because, among other things, they are immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers and/or any utility of such practices is outweighed by the harm caused to consumers. Intel's practices violate the legislative policies of the underlying statutes alleged herein: namely, protecting consumers and preventing persons from being injured. Intel's practices caused substantial injury to Plaintiffs and absent members of the Class and are not outweighed by any benefits, and Plaintiffs and absent members of the Class could not have reasonably avoided their injuries.

434. Intel has engaged in "unlawful" business acts or practices by violating multiple state laws, including the CLRA, Cal. Civ. Code § 1780 *et seq.*, and California common law, as alleged herein.

435. Intel has engaged in fraudulent acts or practices by concealing and/or failing to disclose material facts to Plaintiffs and Class members, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential

information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

436. Intel's fraudulent acts or practices were likely to deceive reasonable consumers.

437. As a result of Defendant's unfair acts or business practices, Plaintiffs and absent Class members have suffered injury in fact and lost money or property.

438. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law, including restitution stemming from Intel's unfair, unlawful, and fraudulent business practices; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

NATIONWIDE COUNT IV

VIOLATIONS OF CALIFORNIA'S FALSE ADVERTISING LAW

Cal. Bus. & Prof. Code § 17500 *et seq.*

439. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

440. Plaintiffs bring this cause of action for themselves and on behalf of the Class and/or on behalf of the California Subclass.

441. Intel's acts and practices, as described herein, have deceived and/or are likely to continue to deceive Class members and the public. As detailed above, Intel misrepresented the CPUs as secure and fast performing in a longstanding advertising campaign, yet failed to disclose material facts, including but not limited to, that: (i) the CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information, (iii) mitigations to address the

Defects would result in significant CPU performance degradation, and (iv) and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

442. For decades, Intel has disseminated uniform advertisements, representations and statements that its CPUs are secure, powerful and fast performing. These uniform advertisements, representations and statements emanated from California and are governed by California law. The advertising, representations and statements were, by their very nature, unfair, deceptive, untrue, and misleading within the meaning of Cal. Bus. & Prof. Code § 17500 *et seq.* Intel's advertisements, representations, and statements promising security, power and fast processor performance, as alleged herein, were misleading, because its CPUs could never be as fast or as powerful as designed and advertised once mitigations addressing the Defects are installed. Such advertisements were intended to, and likely did, deceive the consuming public for the reasons detailed herein.

443. Unless abated, Intel's continued advertising, representations and statements that its CPUs are secure, powerful and fast performing, without disclosing that additional mitigations will be necessary to address ongoing and newly discovered exploits and that such mitigations will result in further performance degradation, will mislead consumers into believing that they are receiving the benefit of their bargain and that the price paid for the CPU is not inflated based upon false promises or assurances.

444. The above-described false, misleading, and deceptive advertising that Intel disseminated continues to have a likelihood to deceive in that Intel concealed and/or failed to disclose material facts, including that: (i) CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; and (iii) mitigations to address the Defects would result in significant CPU performance degradation.

445. Intel has continued to misrepresent to consumers that its CPUs were becoming faster and faster, without explanation of the security shortcuts it took to ensure device performance and speed. Had Intel disclosed those issues, rather than falsely advertising the CPUs' properties, consumers would have not purchased or would have paid significantly less for the CPUs.

446. In making and disseminating the statements alleged herein, Intel knew, or should have known, that its representations, advertisements, and statements were untrue and misleading in violation of California law. Plaintiffs and absent Class members based their purchasing decisions on Intel's representations and omitted material facts. The revenues to Intel attributable to products sold in those false and misleading advertisements amount to hundreds of millions of dollars.

447. The misrepresentations and non-disclosures by Intel of the material facts described and detailed herein constitute false and misleading advertising and, therefore, constitute violations of Cal. Bus. & Prof Code § 17500 *et seq.*

448. As a result of Defendant's unfair business practices, Plaintiffs and absent Class members have suffered injury in fact and lost money or property.

449. Plaintiffs and absent Class members seek all monetary and non-monetary relief allowed by law, including restitution stemming from Intel's business practices; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

NATIONWIDE COUNT V

QUASI CONTRACT OR UNJUST ENRICHMENT

Common Law Claim

450. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

451. Plaintiffs bring this cause of action for themselves and on behalf of the Class and/or on behalf of each state subclass under the law of each state in which Class or subclass members purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU.

452. Plaintiffs and absent Class members purchased Intel CPUs or devices containing Intel CPUs that Intel advertised as secure, powerful and fast performing. To gain a market advantage over its competitors, and unbeknownst to consumers, Intel knowingly sacrificed security for speed and implemented speculative execution in a defective manner. Intel knew that the manner in which it implemented speculative execution would leave the CPUs vulnerable to the Intel CPU exploits. Defendant had knowledge of methods for designing its CPUs to eliminate the threat of the Intel CPU exploits. Defendant chose not to disclose the Defects and resulting exploits; nor did it redesign its CPUs to avoid reduced profits.

453. If Intel had not concealed and/or failed to disclose material facts to Class members, including that, in designing its CPUs, it failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Plaintiffs and absent Class members either would not have bought the CPUs (or devices containing the CPUs), or would have paid less for such products.

454. As a result, Intel was unjustly enriched by the purchase price of those CPUs to the detriment of Plaintiffs and absent Class members.

455. Consequently, Plaintiffs and absent Class members are entitled to restitution in the amount by which Intel was unjustly enriched, to be determined at trial.

CLAIMS ALLEGED ON BEHALF OF THE SUBCLASSES

ALABAMA SUBCLASS COUNT VI

ALABAMA DECEPTIVE TRADE PRACTICES ACT

Ala. Code § 8-19-1 *et seq*.

456. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

457. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Alabama, and/or on behalf of the Alabama Subclass.

458. Intel is a "person" as defined by Ala. Code § 8-19-3(5).

459. Plaintiffs and Alabama Subclass members[145] are "consumers" as defined by Ala. Code § 8-19-3(2).

460. Intel received notice pursuant to Ala. Code § 8-19-10(e) concerning its wrongful conduct as alleged herein by Plaintiffs and Alabama Subclass members. Sending pre-suit notice pursuant to Ala. Code § 8-19-10(e), however, would have been an exercise in futility for Plaintiffs, because Intel has already been informed of the allegedly unfair and unlawful conduct as described

[145] Unless otherwise noted, references throughout this Amended Complaint to a state subclass or to the members of a particular state subclass (e.g., "Alabama Subclass members" or "the Florida Subclass") alternatively refer to the members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in that state.

herein as of the date of the first-filed lawsuit, and has yet to offer Alabama Subclass members a remedy in accordance with similar consumer protection statutes.

461. Intel advertised, offered, or sold goods or services in Alabama, and engaged in trade or commerce directly or indirectly affecting the people of Alabama.

462. Intel engaged in deceptive acts and practices in the conduct of trade or commerce, in violation of the Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5, including:

463. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with the Defects, which go toward their central functionality, resulting in security risks, compromising consumer data, and—if patched—significantly degrading CPU performance thereby, again, impacting their central functionality, so that consumers did not receive the benefit of their bargain;

464. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, therefore, putting profits over the safety of consumer data;

465. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

466. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that security is a priority in its devices;

467. Making affirmative public representations about the speed of Intel CPUs while knowing that, in order for those CPUs to offer security for consumers' data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

468. Concealing and/or failing to disclose material facts, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU

performance degradation, and that in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

469. Intel's representations and omissions were material because they were likely to deceive ordinary, reasonable consumers.

470. Intel intended to mislead Plaintiffs and Alabama Subclass members and induce them to rely on its misrepresentations and omissions.

471. Had Intel disclosed to Plaintiffs and Alabama Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information, (iii) mitigations to address the Defects would result in significant CPU performance degradation, and (iv) that in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Alabama Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

472. Intel acted intentionally, knowingly, and maliciously to violate the Alabama Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs' and Alabama Subclass members' rights. Intel's knowledge of the CPUs' Defects put it on notice that the CPUs were not as it advertised.

473. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and Alabama Subclass members have suffered and will continue to suffer injury, ascertainable losses of

money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and safety issues.

474. Intel's deceptive acts and practices caused substantial injury to Plaintiffs and Alabama Subclass members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

475. Plaintiffs and the Alabama Subclass seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages, or (b) statutory damages of $100 each; treble damages; injunctive relief; attorneys' fees; costs; and any other relief that is just and proper.

ALASKA SUBCLASS COUNT VII

ALASKA CONSUMER PROTECTION ACT

Alaska Stat. § 45.50.471 *et seq*.

476. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

477. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Alaska, and/or on behalf of the Alaska Subclass.

478. Subclass, repeats and re-alleges all previously alleged paragraphs, as if fully alleged herein.

479. Intel advertised, offered, or sold goods or services in Alaska and engaged in trade or commerce directly or indirectly affecting the people of Alaska.

480. Alaska Subclass members are "consumers" as defined by Alaska Stat. § 45.50.561(4).

481. Intel received notice pursuant to Alaska Stat. § 45.50.535 concerning its wrongful conduct as alleged herein by Plaintiffs and Alaska Subclass members. Sending pre-suit notice pursuant to Alaska Stat. § 45.50.535, however, is an exercise in futility for Plaintiffs, because Intel has already been informed of the allegedly unfair and unlawful conduct as described herein as of the date of the first-filed lawsuit, and has yet to offer Alaska Subclass members remedy in accordance with similar consumer protection statutes.

482. Intel engaged in unfair or deceptive acts and practices in the conduct of trade or commerce, in violation Alaska Stat. § 45.50.471, including:

483. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with the Defects, which go toward their central functionality, resulting in security risks, compromising confidential information, and—if patched—significantly degrading CPU performance thereby, again, impacting their central functionality, so that consumers did not receive the benefit of their bargain;

484. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, therefore, putting profits over the safety of consumer data;

485. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

486. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

487. Making affirmative public representations about the speed of Intel CPUs while knowing that, in order for those CPUs to offer security for consumers' data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

488. Concealing and/or failing to disclose material facts, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

489. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

490. Intel intended to mislead Plaintiffs and Alaska Subclass members and induce them to rely on its misrepresentations and omissions.

491. Intel acted intentionally, knowingly, and maliciously to violate Alaska's Consumer Protection Act, and recklessly disregarded Plaintiffs' and Alaska Subclass members' rights. Intel's knowledge of the CPU's security and performance issues put it on notice that the CPUs were not as it advertised.

492. As a direct and proximate result of Intel's unfair and deceptive acts and practices, Plaintiffs and Alaska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain, and increased time and expense in dealing with CPU performance and security issues.

493. Plaintiffs and the Alaska Subclass seek all monetary and non-monetary relief allowed by law, including the greater of (a) three times their actual damages, or (b) statutory damages in the amount of $500; punitive damages; reasonable attorneys' fees and costs; injunctive relief; and any other relief that is necessary and proper.

ARIZONA SUBCLASS COUNT VIII

ARIZONA CONSUMER FRAUD ACT

A.R.S. § 44-1521 *et seq*.

494. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

495. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Arizona, and/or on behalf of the Arizona Subclass.

496. Intel is a "person" as defined by A.R.S. § 44-1521(6).

497. Intel advertised, offered, or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

498. Intel engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Arizona in connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5)) in violation of A.R.S. § 44-1522(A).

499. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

500. Intel intended to mislead Plaintiffs and Arizona Subclass members and induce them to rely on its misrepresentations and omissions.

501. Had Intel disclosed to Plaintiffs and Arizona Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel had failed to

take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Arizona Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

502. Intel acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiffs' and Arizona Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

503. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and Arizona Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and safety issues.

504. Plaintiffs and Arizona Subclass members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

ARKANSAS SUBCLASS COUNT IX

ARKANSAS DECEPTIVE TRADE PRACTICES ACT,

A.C.A. § 4-88-101, *et seq*.

505. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

506. Plaintiffs bring this count on behalf of themselves and all members of theClass that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Arkansas, and/or on behalf of the Arkansas Subclass.

507. Intel is a "person" as defined by A.C.A. § 4-88-102(5).

508. Intel's products and services are "goods" and "services" as defined by A.C.A. §§ 4-88-102(4) and (7).

509. Intel advertised, offered, or sold goods or services in Arkansas and engaged in trade or commerce directly or indirectly affecting the people of Arkansas.

510. The Arkansas Deceptive Trade Practices Act ("ADTPA"), A.C.A. § 4-88-101 *et seq.*, prohibits unfair, deceptive, false, and unconscionable trade practices.

511. Intel engaged in acts of deception and false pretense in connection with the sale and advertisement of services in violation of A.C.A. § 4-88-1-8(1) and concealment, suppression and omission of material facts, with intent that others rely upon the concealment, suppression or omission in violation of A.C.A. § 4-88-1-8(2), and engaged in the following deceptive and unconscionable trade practices defined in A.C.A. § 4-88-107:

512. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with the Defects, which go toward their central functionality, resulting in security risks, compromising confidential information, and—if patched—significantly degrading CPU performance thereby, again, impacting their central functionality, so that consumers did not receive the benefit of their bargain;

513. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, therefore, putting profits over the safety of consumer data;

514. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

515. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

516. Making affirmative public representations about the speed of Intel CPUs while knowing that, in order for those CPUs to offer security for consumers' data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

517. Concealing and/or failing to disclose material facts, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

518. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

519. Intel intended to mislead Plaintiffs and Arkansas Subclass members and induce them to rely on its misrepresentations and omissions.

520. Had Intel disclosed to Plaintiffs and Arkansas Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were

continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Arkansas Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

521. Intel acted intentionally, knowingly, and maliciously to violate Arkansas's Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs' and Arkansas Subclass members' rights. Intel's knowledge of the CPU's performance and safety issues put it on notice that the CPUs were not as it advertised.

522. As a direct and proximate result of Intel's unconscionable, unfair, and deceptive acts or practices and Plaintiffs and Arkansas Subclass members' reliance thereon, Plaintiffs and Arkansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and safety.

523. Plaintiffs and the Arkansas Subclass members seek all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

COLORADO SUBCLASS COUNT X

COLORADO CONSUMER PROTECTION ACT,

Colo. Rev. Stat. § 6-1-101 *et seq*.

524. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

525. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Colorado, and/or on behalf of the Colorado Subclass.

526. Intel is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6).

527. Intel engaged in "sales" as defined by Colo. Rev. Stat. § 6-1-102(10).

528. Plaintiffs and Colorado Subclass members, as well as the general public, are actual or potential consumers of the products and services offered by Intel or successors in interest to actual consumers.

529. Intel engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

530. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with the Defects, which go toward their central functionality, resulting in security risks, compromising confidential information, and—if patched—significantly degrading CPU performance thereby, again, impacting their central functionality, so that consumers did not receive the benefit of their bargain;

531. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, therefore, putting profits over the safety of consumer data;

532. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

533. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

534. Making affirmative public representations about the speed of Intel CPUs while knowing that, in order for those CPUs to offer security for consumers' data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

535. Concealing and/or failing to disclose material facts, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

536. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

537. Intel intended to mislead Plaintiffs and Colorado Subclass members and induce them to rely on its misrepresentations and omissions.

538. Had Intel disclosed to Plaintiffs and Colorado Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that, in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Colorado Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

539. Intel acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Plaintiffs' and Colorado Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

540. As a direct and proximate result of Intel's deceptive trade practices, Colorado Subclass members suffered injuries to their legally protected interests.

541. Intel's deceptive trade practices significantly impact the public because Intel is one of the largest CPU manufacturers in the world, with hundreds of thousands of sales of those devices to Colorado consumers.

542. Plaintiffs and Colorado Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages, (b) $500 each, or (c) three times actual damages (for Intel's bad faith conduct); injunctive relief; and reasonable attorneys' fees and costs.

CONNECTICUT SUBCLASS COUNT XI

CONNECTICUT TRADE PRACTICES ACT

C.G.S.A. § 42-110g *et seq*.

543. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

544. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Connecticut, and/or on behalf of the Connecticut Subclass.

545. Intel is a "person" as defined by C.G.S.A. § 42-110a (3).

546. Intel is engaged in "trade" or "commerce" as those terms are defined by C.G.S.A. § 42-110a(4).

547. At the time of filing the Complaint, Plaintiffs sent notice to the Attorney General and Commissioner of Consumer Protection pursuant to C.G.S.A. § 42-110g(c). Plaintiffs will provide a file-stamped copy of the Complaint to the Attorney General and Commissioner of Consumer Protection.

548. Intel advertised, offered, or sold goods or services in Connecticut, and engaged in trade or commerce directly or indirectly affecting the people of Connecticut.

549. Intel engaged in deceptive acts and practices and unfair acts and practices in the conduct of trade or commerce, in violation of the C.G.S.A. § 42-110b, including:

550. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with the Defects, which go toward their central functionality, resulting in security risks, compromising confidential information, and—if patched—significantly degrading CPU performance thereby, again, impacting their central functionality, so that consumers did not receive the benefit of their bargain;

551. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, therefore, putting profits over the safety of consumer data;

552. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

553. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

554. Making affirmative public representations about the speed of Intel CPUs while knowing that, in order for those CPUs to offer security for consumers' data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

555. Concealing and/or failing to disclose material facts, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

556. Intel intended to mislead Plaintiffs and Connecticut Subclass members and induce them to rely on its misrepresentations and omissions.

557. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

558. Intel's representations and omissions were material because were likely to deceive reasonable consumers.

559. Had Intel disclosed to Plaintiffs and Connecticut Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result

in significant CPU performance degradation; and (iv) that, in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Connecticut Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

560. Intel acted intentionally, knowingly, and maliciously to violate the Connecticut Unfair Trade Practices Act, and recklessly disregarded Plaintiffs' and Connecticut Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

561. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and Connecticut Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with CPU performance and security issues.

562. Intel's deceptive acts and practices caused substantial, ascertainable injury to Plaintiffs and Connecticut Subclass members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

563. Intel's violations of Connecticut law were done with reckless indifference to Plaintiffs and the Connecticut Subclass or was with an intentional or wanton violation of those rights.

564. Plaintiffs request damages in the amount to be determined at trial, including statutory and common law damages, attorneys' fees, and punitive damages.

DELAWARE SUBCLASS COUNT XII

DELAWARE CONSUMER FRAUD ACT

6 Del. Code § 2513 *et seq.*

565. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

566. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Delaware, and/or on behalf of the Delaware Subclass.

567. Intel is a "person" that is involved in the "sale" of "merchandise," as defined by 6 Del. Code § 2511(6)-(8).

568. Intel advertised, offered, or sold goods or services in Delaware and engaged in trade or commerce directly or indirectly affecting the people of Delaware.

569. Intel used and employed deception, fraud, false pretense, false promise, misrepresentation, and the concealment, suppression, and omission of material facts with intent that others rely upon such concealment, suppression and omission, in connection with the sale and advertisement of merchandise, in violation of 6 Del. Code § 2513(a).

570. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

571. Intel acted intentionally, knowingly, and maliciously to violate Delaware's Consumer Fraud Act, and recklessly disregarded Plaintiffs' and Delaware Subclass members'

rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

572. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

573. Had Intel disclosed to Plaintiffs and Delaware Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that, in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Delaware Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

574. Intel's unlawful trade practices were gross, oppressive, and aggravated, and Intel breached the trust of Plaintiffs and Delaware Subclass members.

575. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Delaware Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

576. Plaintiffs and Delaware Subclass members seek all monetary and non-monetary relief allowed by law, including damages under 6 Del. Code § 2525 for injury resulting from the direct and natural consequences of Intel's unlawful conduct; injunctive relief; and reasonable attorneys' fees and costs.

DISTRICT OF COLUMBIA SUBCLASS COUNT XIII

DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT

D.C. Code § 28-3904 *et seq.*

577. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

578. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in the District of Columbia, and/or on behalf of the District of Columbia Subclass.

579. Intel is a "person" as defined by D.C. Code § 28-3901(a)(1).

580. Intel is a "merchant" as defined by D.C. Code § 28-3901(a)(3).

581. Plaintiffs and District of Columbia Subclass members are "consumers" who purchased or received goods or services for personal, household, or family purposes, as defined by D.C. Code § 28-3901.

582. Intel advertised, offered, or sold goods or services in District of Columbia and engaged in trade or commerce directly or indirectly affecting the people of District of Columbia.

583. Intel engaged in unfair, unlawful, and deceptive trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of D.C. Code § 28-3904, including:

584. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with the Defects, which go toward their central functionality, resulting in security risks, compromising confidential information, and—if patched—significantly degrading CPU performance thereby, again, impacting their central functionality, so that consumers did not receive the benefit of their bargain;

585. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, therefore, putting profits over the safety of consumer data;

586. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

587. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

588. Making affirmative public representations about the speed of Intel CPUs while knowing that, in order for those CPUs to offer security for consumers' data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

589. Concealing and/or failing to disclose material facts, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

590. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

591. Intel intended to mislead Plaintiffs and District of Columbia Subclass members and induce them to rely on its misrepresentations and omissions.

592. The above unfair and deceptive practices and acts by Intel were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and District of Columbia Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

593. Intel acted intentionally, knowingly, and maliciously to violate the District of Columbia's Consumer Protection Procedures Act, and recklessly disregarded Plaintiffs' and District of Columbia Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

594. As a direct and proximate result of Intel's unfair, unlawful, and deceptive trade practices, Plaintiffs and absent District of Columbia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with CPU performance and security issues.

595. Plaintiffs and District of Columbia Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, injunctive relief, punitive damages, attorneys' fees and costs, the greater of treble damages or $1500 per violation, and any other relief that the Court deems proper.

FLORIDA SUBCLASS COUNT XIV

FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT

Fla. Stat. § 501.201 *et seq.*

596. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

597. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Florida, and/or on behalf of the Florida Subclass.

598. Plaintiffs and Florida Subclass members are "consumers" as defined by Fla. Stat. § 501.203.

599. Intel advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

600. Intel engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1).

601. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

602. Had Intel disclosed to Plaintiffs and Florida Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result

in significant CPU performance degradation; and (iv) that, in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Florida Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

603. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Florida Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

604. Plaintiffs and Florida Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.21; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

GEORGIA SUBCLASS COUNT XV

GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT

O.C.G.A. § 10-1-390 *et seq.*

605. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

606. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Georgia, and/or on behalf of the Georgia Subclass.

607. Intel, Plaintiffs, and Georgia Subclass members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

608. Intel received notice pursuant to O.C.G.A. § 10-1-399 concerning its wrongful conduct as alleged herein by Plaintiffs and Georgia Subclass members. Sending pre-suit notice pursuant to O.C.G.A. § 10-1-399, however, is an exercise in futility for Plaintiffs because Intel has already been informed of the allegedly unfair and unlawful conduct as described herein as of the date of the first-filed lawsuit and has yet to offer Georgia Subclass members remedy.

609. Intel engaged in deceptive trade practices in the conduct of its business, in violation of O.C.G.A. § 10-1-372(a), including:

610. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with the Defects, which go toward their central functionality, resulting in security risks, compromising confidential information, and—if patched—significantly degrading CPU performance thereby, again, impacting their central functionality, so that consumers did not receive the benefit of their bargain;

611. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, therefore, putting profits over the safety of consumer data;

612. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

613. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

614. Making affirmative public representations about the speed of Intel CPUs while knowing that, in order for those CPUs to offer security for consumers' data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

615. Concealing and/or failing to disclose material facts, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

616. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

617. Intel intended to mislead Plaintiffs and Georgia Subclass members and induce them to rely on its misrepresentations and omissions.

618. In the course of its business, Intel engaged in activities with a tendency or capacity to deceive.

619. Intel acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs' and Georgia Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

620. Had Intel disclosed to Plaintiffs and Georgia Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that, in designing its CPUs, Intel had failed to

take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Georgia Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

621. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Georgia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

622. Plaintiffs and Georgia Subclass members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under O.C.G.A. § 10-1-373.

HAWAII SUBCLASS COUNT XI

HAWAII UNFAIR PRACTICES AND UNFAIR COMPETITION ACT

Haw. Rev. Stat. § 480-1 *et seq.*

623. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

624. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Hawaii, and/or on behalf of the Hawaii Subclass.

625. Plaintiffs and Hawaii Subclass members are "consumers" as defined by Haw. Rev. Stat. § 480-1.

626. Plaintiffs, Hawaii Subclass members, and Intel are "persons" as defined by Haw. Rev. Stat. § 480-1.

627. Intel advertised, offered, or sold goods or services in Hawaii and engaged in trade or commerce directly or indirectly affecting the people of Hawaii.

628. Intel engaged in unfair or deceptive acts or practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods and services purchased by Hawaii Subclass members in violation of Haw. Rev. Stat. § 480-2(a).

629. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

630. Intel intended to mislead Plaintiffs and Hawaii Subclass members and induce them to rely on its misrepresentations and omissions.

631. The foregoing unlawful and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous.

632. Intel acted intentionally, knowingly, and maliciously to violate Hawaii's Unfair Practices and Unfair Competition Act, and recklessly disregarded Plaintiffs' and Hawaii Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

633. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Hawaii Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

634. Plaintiffs and Hawaii Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, benefit of the bargain damages, treble damages, injunctive relief, and reasonable attorneys' fees and costs.

HAWAII SUBCLASS COUNT XII

HAWAII UNIFORM DECEPTIVE TRADE PRACTICE ACT

Haw. Rev. Stat. § 481A-3 *et seq.*

635. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

636. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Hawaii, and/or on behalf of the Hawaii Subclass.

637. Plaintiffs and Hawaii Subclass members are "persons" as defined by Haw. Rev. Stat. § 481A-2.

638. Intel engaged in unfair and deceptive trade practices in the conduct of its business, violating Haw. Rev. Stat. § 481A-3, including:

639. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with the Defects, which go toward their central functionality, resulting in security risks, compromising confidential information, and—if patched—significantly degrading CPU performance thereby, again, impacting their central functionality, so that consumers did not receive the benefit of their bargain;

640. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

641. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

642. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

643. Making affirmative public representations about the speed of Intel CPUs while knowing that, in order for those CPUs to offer security for consumers' data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

644. Concealing and/or failing to disclose material facts, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

645. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

646. The above unfair and deceptive practices and acts by Intel were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Hawaii Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

647. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Hawaii Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

648. Plaintiffs and Hawaii Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, attorneys' fees and costs, and any other relief that the Court deems proper.

IDAHO SUBCLASS COUNT XIII

IDAHO CONSUMER PROTECTION ACT

Idaho Code § 48-601 *et seq.*

649. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

650. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Idaho, and/or on behalf of the Idaho Subclass.

651. Intel is a "person" as defined by Idaho Code § 48-602(1).

652. Intel's conduct as alleged herein pertained to "goods" and "services" as defined by Idaho Code § 48-602(6) and (7).

653. Intel advertised, offered, or sold goods or services in Idaho and engaged in trade or commerce directly or indirectly affecting the people of Idaho.

654. Intel engaged in unfair and deceptive acts or practices, and unconscionable acts and practices, in the conduct of trade and commerce with respect to the sale and advertisement of goods and services, in violation of Idaho Code §§ 48-603 and 48-603(C), including:

655. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with the Defects, which go toward their central functionality, resulting in security risks, compromising confidential information, and—if patched—significantly degrading CPU

performance thereby, again, impacting their central functionality, so that consumers did not receive the benefit of their bargain;

656. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

657. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

658. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

659. Making affirmative public representations about the speed of Intel CPUs while knowing that, in order for those CPUs to offer security for consumers' data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

660. Concealing and/or failing to disclose material facts, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

661. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

662. Intel intended to mislead Plaintiffs and Idaho Subclass members and induce them to rely on its misrepresentations and omissions. Intel knew its representations and omissions were false.

663. Intel acted intentionally, knowingly, and maliciously to violate Idaho's Consumer Protection Act, and recklessly disregarded Plaintiffs' and Idaho Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

664. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Idaho Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

665. Plaintiffs and Idaho Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, injunctive relief, costs, and attorneys' fees.

ILLINOIS SUBCLASS COUNT XIV

ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT

815 ILCS § 505 *et seq.*

666. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

667. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Illinois, and/or on behalf of the Illinois Subclass.

668. Intel is a "person" as defined by 815 ILCS §§ 505/1(c).

669. Plaintiffs and Illinois Subclass members are "consumers" as defined by 815 ILCS §§ 505/1(e).

670. Intel's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 ILCS § 505/1(f). Intel's conduct is described in full detail above.

671. Intel's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 ILCS § 505/2.

672. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

673. Intel intended to mislead Plaintiffs and Illinois Subclass members and induce them to rely on its misrepresentations and omissions.

674. The above unfair and deceptive practices and acts by Intel were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefit to consumers or to competition.

675. Intel acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiffs' and Illinois Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

676. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issue.

677. Plaintiffs and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

ILLINOIS SUBCLASS COUNT XV

ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT

815 ILCS § 510/2 *et seq.*

678. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

679. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Illinois, and/or on behalf of the Illinois Subclass.

680. Intel is a "person" as defined by 815 ILCS §§ 510/1(5).

681. Intel engaged in deceptive trade practices in the conduct of its business, in violation of 815 ILCS §§ 510/2(a), including:

682. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with the Defects, which go toward their central functionality resulting in security risks, compromising confidential information, and—if patched—significantly degrading CPU performance thereby, again, impacting their central functionality, so that consumers did not receive the benefit of their bargain;

683. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

684. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

685. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

686. Making affirmative public representations about the speed of Intel CPUs while knowing that, in order for those CPUs to offer security for consumers' data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

687. Concealing and/or failing to disclose material facts, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

688. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

689. The above unfair and deceptive practices and acts by Intel were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Illinois Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

690. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

691. Plaintiffs and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

INDIANA SUBCLASS COUNT XVI

INDIANA DECEPTIVE CONSUMER SALES ACT

Ind. Code § 24-5-0.5-1 *et seq.*

692. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

693. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Indiana, and/or on behalf of the Indiana Subclass.

694. Intel is a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

695. Intel is a "supplier" as defined by § 24-5-0.5-2(a)(1), because it regularly engages in or solicits "consumer transactions" within the meaning of § 24-5-0.5-2(a)(3)(A).

696. Intel engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

697. Intel's representations and omissions include both implicit and explicit representations and were carried out as a scheme or artifice to defraud.

698. Intel's acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

699. The injury to consumers from Intel's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

700. Consumers could not have reasonably avoided injury because Intel's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the performance and security of its CPUs, and Defects within those processors, Intel created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

701. Intel's business practices, in concealing material information or misrepresenting the qualities, characteristics, and performance of its CPUs, had no countervailing benefit to consumers or to competition.

702. Intel's acts and practices were "abusive" for numerous reasons, including: (a) because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction, interfering with consumers' decision-making; (b) because they took unreasonable advantage of consumers' lack of understanding about the material risks, costs, or conditions of a consumer transaction; consumers lacked an understanding of the material risks and costs of a variety of their transactions; (c) because they took unreasonable advantage of consumers' inability to protect their own interests; consumers could not protect their interests due to the asymmetry in information between them and Intel; (d) because Intel took unreasonable advantage of consumers' reasonable reliance that it was providing truthful and accurate information.

703. Intel also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including: (a) misrepresenting that the subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have; (b) misrepresenting that the subject of a consumer transaction is of a particular standard, quality,

grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not; and (c) misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (here, greater speed) than the supplier intends or reasonably expects.

704. Intel intended to mislead Plaintiffs and Indiana Subclass members and induce them to rely on its misrepresentations and omissions.

705. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

706. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

707. Had Intel disclosed to Plaintiffs and Indiana Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information, (iii) mitigations to address the Defects would result in significant CPU performance degradation, and (iv) that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs

that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Indiana Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

708. Intel acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act, and recklessly disregarded Plaintiffs' and Indiana Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

709. Intel received notice pursuant to Ind. Code § 24-5-0.5-5 concerning its wrongful conduct as alleged herein by Plaintiffs and Indiana Subclass members. Moreover, Intel has had constructive notice of Plaintiffs' demand for relief for the Indiana Subclass pursuant to Ind. Code § 24-5-0.5-5 since the filing of the first action among those that have now been centralized in this multidistrict litigation, which contained substantially similar allegations. Therefore, sending pre-suit notice pursuant to Ind. Code § 24-5-0.5-5 is an exercise in futility for Plaintiffs because Intel has not cured its unfair, abusive, and deceptive acts and practices, or its violations of Indiana Deceptive Consumer Sales Act were incurable.

710. Intel's conduct includes incurable deceptive acts that Intel engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5-0.5-2(a)(8).

711. As a direct and proximate result of Intel's uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiffs and absent Indiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with CPU performance and security issues.

712. Intel's violations present a continuing risk to Plaintiffs and absent Indiana Subclass members as well as to the general public.

713. Plaintiffs and Indiana Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $500 for each non-willful violation; the greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

IOWA SUBCLASS COUNT XVII

IOWA PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT

Iowa Code § 714H

714. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

715. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Iowa, and/or on behalf of the Iowa Subclass.

716. Intel is a "person" as defined by Iowa Code § 714H.2(7).

717. Plaintiffs and Iowa Subclass members are "consumers" as defined by Iowa Code § 714H.2(3).

718. Intel's conduct described herein related to the "sale" or "advertisement" of "merchandise" as defined by Iowa Code §§ 714H.2(2), (6), & (8).

719. Intel engaged in unfair, deceptive, and unconscionable trade practices, in violation of the Iowa Private Right of Action for Consumer Frauds Act, as described throughout and herein.

720. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

721. Intel intended to mislead Plaintiffs and Iowa Subclass members and induce them to rely on its misrepresentations and omissions.

722. Intel acted intentionally, knowingly, and maliciously to violate Iowa's Private Right of Action for Consumer Frauds Act, and recklessly disregarded Plaintiffs' and Iowa Subclass members' rights. Intel's knowledge of the CPU performance and security issues put it on notice that the CPUs were not as it advertised.

723. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Iowa Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues

724. Plaintiffs has provided the requisite notice to the Iowa Attorney General, the office of which approved the filing of this class action lawsuit pursuant to Iowa Code § 714H.7.

725. Plaintiffs and Iowa Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, punitive damages, and reasonable attorneys' fees and costs.

KANSAS SUBCLASS COUNT XVIII

KANSAS CONSUMER PROTECTION ACT

K.S.A. § 50-623 *et seq.*

726. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

727. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Kansas, and/or on behalf of the Kansas Subclass.

728. K.S.A. § 50-623 *et seq.* is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

729. Plaintiffs and Kansas Subclass members are "consumers" as defined by K.S.A. § 50-624(b).

730. The acts and practices described herein are "consumer transactions," as defined by K.S.A. § 50-624(c).

731. Intel is a "supplier" as defined by K.S.A. § 50-624(l).

732. Intel advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

733. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

734. Intel intended to mislead Plaintiffs and Kansas Subclass members and induce them to rely on its misrepresentations and omissions.

735. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or

superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

736. Had Intel disclosed to Plaintiffs and Kansas Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that, in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Kansas Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

737. Intel also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including knowingly taking advantage of the inability of Plaintiffs and the Kansas Subclass to reasonably protect their interests, due to their lack of knowledge (*see* K.S.A. § 50-627(b)(1)); and requiring Plaintiffs and absent Kansas Subclass members to enter into a consumer transaction on terms that Intel knew were substantially one-sided in favor of Intel (*see* K.S.A. § 50-627(b)(5)).

738. Plaintiffs and absent Kansas Subclass members had unequal bargaining power with respect to their purchase and/or use of Intel's CPUs because of Intel's omissions and misrepresentations.

739. The above unfair, deceptive, and unconscionable practices and acts by Intel were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and absent Kansas Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

740. Intel acted intentionally, knowingly, and maliciously to violate Kansas's Consumer Protection Act, and recklessly disregarded Plaintiffs' and Kansas Subclass members' rights. Intel's knowledge of the CPUs' security and performance issue put it on notice that the CPUs were not as it advertised.

741. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Kansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

742. Plaintiffs and Kansas Subclass members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636; injunctive relief; and reasonable attorneys' fees and costs.

LOUISIANA SUBCLASS COUNT XIX

LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW

La. Rev. Stat. Ann. § 51:1401 *et seq.*

743. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

744. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Louisiana, and/or on behalf of the Louisiana Subclass.

745. Intel, Plaintiffs, and Louisiana Subclass members are "persons" within the meaning of the La. Rev. Stat. Ann. § 51:1402(8).

746. Plaintiffs and Louisiana Subclass members are "consumers" within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

747. Intel engaged in "trade" or "commerce" within the meaning of La. Rev. Stat. Ann. § 51:1402(10).

748. The Louisiana Unfair Trade Practices and Consumer Protection Law ("Louisiana CPL") makes unlawful "unfair or deceptive acts or practices in the conduct of any trade or commerce." La. Rev. Stat. Ann. § 51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

749. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

750. Intel intended to mislead Plaintiffs and Louisiana Subclass members and induce them to rely on its misrepresentations and omissions.

751. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects; that the CPU Defects allowed unauthorized access to confidential information; that necessary mitigations to address the Defects would result in significant CPU performance degradation; and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because

both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

752. Intel's unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and absent Louisiana Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

753. Intel acted intentionally, knowingly, and maliciously to violate Louisiana's Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiffs' and Louisiana Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

754. Had Intel disclosed to Plaintiffs and Louisiana Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Louisiana Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

755. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

756. Plaintiffs and Louisiana Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages; treble damages for Intel's knowing violations of the Louisiana CPL; declaratory relief; attorneys' fees; and any other relief that is just and proper.

MAINE SUBCLASS COUNT XX

MAINE UNFAIR TRADE PRACTICES ACT

5 Me. Rev. Stat. §§ 205, 213, *et seq.*

757. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

758. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Maine, and/or on behalf of the and/or the Maine Subclass.

759. Intel is a "person" as defined by 5 Me. Stat. § 206(2).

760. Intel's conduct as alleged herein related was in the course of "trade and commerce" as defined by 5 Me. Stat. § 206(3).

761. Plaintiffs and Maine Subclass members purchased goods and/or services for personal, family, and/or household purposes.

762. A demand for relief in the form substantially similar to that required by 5 Me. Rev. Stat. § 213(1-A) was already sent at the commencement of this lawsuit but Intel has not made a

written tender of settlement or offer of judgment. Intel received supplemental notice pursuant to 5 Me. Rev. Stat. § 213(1-A) concerning its wrongful conduct as alleged herein by Plaintiffs and Maine Subclass members, but this and any subsequent demand was and would be an exercise in futility.

763. Intel engaged in unfair and deceptive trade acts and practices in the conduct of trade or commerce, in violation of 5 Me. Rev. Stat. §207.

764. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

765. Had Intel disclosed to Plaintiffs and Maine Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Maine Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

766. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Maine Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

767. Plaintiffs and the Maine Subclass members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive and other equitable relief, and attorneys' fees and costs.

MAINE SUBCLASS COUNT XXI

MAINE UNIFORM DECEPTIVE TRADE PRACTICES ACT

10 Me. Rev. Stat. § 1212 *et seq.*

768. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

769. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Maine, and/or on behalf of the and/or the Maine Subclass.

770. Intel is a "person" as defined by 10 Me. Rev. Stat. § 1211(5).

771. Intel advertised, offered, or sold goods or services in Maine and engaged in trade or commerce directly or indirectly affecting the people of Maine.

772. Intel engaged in deceptive trade practices in the conduct of its business, in violation of 10 Me. Rev. Stat. § 1212, including: representing that goods or services have characteristics that they do not have; representing that goods or services are of a particular standard, quality, or grade if they are of another; advertising goods or services with intent not to sell them as advertised; and engaging in other conduct that creates a likelihood of confusion or misunderstanding.

773. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

774. Intel intended to mislead Plaintiffs and Maine Subclass members and induce them to rely on its misrepresentations and omissions.

775. Had Intel disclosed to Plaintiffs and Maine Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Maine Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

776. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Maine Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

777. Maine Subclass members are likely to be damaged by Intel's ongoing deceptive trade practices.

778. Plaintiffs and Maine Subclass members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive or other equitable relief, and attorneys' fees and costs.

MARYLAND SUBCLASS COUNT XXII

MARYLAND CONSUMER PROTECTION ACT

Md. Comm. Code § 13-301 *et seq.*

779. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

780. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Maryland, and/or on behalf of the Maryland Subclass.

781. Intel is a person as defined by Md. Comm. Code § 13-101(h).

782. Intel's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Comm. Code §§ 13-101(i) and 13-303.

783. Maryland Subclass members are "consumers" as defined by Md. Comm. Code § 13-101(c).

784. Intel advertises, offers, or sell "consumer goods" or "consumer services" as defined by Md. Comm. Code § 13-101(d).

785. Intel advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

786. Intel engaged in unfair and deceptive trade practices, in violation of Md. Comm. Code § 13-301, including: (a) false or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers; (b) representing that consumer goods or services have a characteristic that they do not have; (c) representing that consumer goods or services are of a particular standard, quality, or grade that they are not; (d) failing to state a material fact where the failure deceives or tends to deceive; (e) advertising or offering consumer

goods or services without intent to sell, lease, or rent them as advertised or offered; (f) deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

787. Intel engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services or with respect to the extension of consumer credit, in violation of Md. Comm. Code § 13-303.

788. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

789. Intel intended to mislead Plaintiffs and Maryland Subclass members and induce them to rely on its misrepresentations and omissions.

790. Had Intel disclosed to Plaintiffs and Maryland Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Maryland Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

791. Intel acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiffs' and Maryland Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

792. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Maryland Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

793. Plaintiffs and Maryland Subclass members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

MICHIGAN SUBCLASS COUNT XXIII

MICHIGAN CONSUMER PROTECTION ACT

Mich. Comp. Laws Ann. § 445.903 *et seq.*

794. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

795. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Michigan, and/or on behalf of the Michigan Subclass.

796. Intel, Plaintiffs, and absent Michigan Subclass members are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

797. Intel advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

798. Intel engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including: (a) representing that its goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c); (b) representing that its goods and services are of a particular standard or quality if they are of another, in violation of Mich. Comp. Laws Ann. § 445.903(1)(e); (c) making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and (d) failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

799. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

800. Intel intended to mislead Plaintiffs and Michigan Subclass members and induce them to rely on its misrepresentations and omissions.

801. Intel acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiffs and Michigan Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

802. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Michigan Subclass members have suffered and will continue to suffer injury, ascertainable

losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

803. Plaintiffs and Michigan Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250 each, injunctive relief, and any other relief that is just and proper.

MINNESOTA SUBCLASS COUNT XXIV

MINNESOTA CONSUMER FRAUD ACT

Minn. Stat. § 325F.68, *et seq.* and Minn. Stat. § 8.31 *et seq.*

804. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

805. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Minnesota, and/or on behalf of the Minnesota Subclass.

806. Intel, Plaintiffs, and the absent members of the Minnesota Subclass are a "person" as defined by Minn. Stat. § 325F.68(3).

807. Intel goods, services, commodities, and intangibles (specifically, Intel CPUs) are "merchandise" as defined by Minn. Stat. § 325F.68(2).

808. Intel engaged in "sales" as defined by Minn. Stat. § 325F.68(4).

809. Intel engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of merchandise, in violation of Minn. Stat. § 325F.69(1), as described herein.

810. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects; that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation; and that, in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

811. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

812. Intel intended to mislead Plaintiffs and Minnesota Subclass members and induce them to rely on its misrepresentations and omissions.

813. Intel's fraudulent, misleading, and deceptive practices affected the public interest, including millions of Minnesotans who purchased and/or used Intel CPUs.

814. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

815. Plaintiffs and Minnesota Subclass members seek all monetary and non-monetary relief allowed by law, including damages, injunctive or other equitable relief, and attorneys' fees, disbursements, and costs.

MINNESOTA SUBCLASS COUNT XXV

MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT

Minn. Stat. § 325D.43 *et seq.*

816. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

817. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Minnesota, and/or on behalf of the Minnesota Subclass.

818. By engaging in deceptive trade practices in the course of its business and vocation, directly or indirectly affecting the people of Minnesota, Intel violated Minn. Stat. § 325D.44, including the following provisions: representing that its goods and services had characteristics, uses, and benefits that they did not have, in violation of Minn. Stat. § 325D.44(1)(5); representing that goods and services are of a particular standard or quality when they are of another, in violation of Minn. Stat. § 325D.44(1)(7); advertising goods and services with intent not to sell them as advertised, in violation of Minn. Stat. § 325D.44(1)(9); and engaging in other conduct that similarly creates a likelihood of confusion or misunderstanding, in violation of Minn. Stat. § 325D.44(1)(13).

819. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

820. Intel intended to mislead Plaintiffs and Minnesota Subclass members and induce them to rely on its misrepresentations and omissions.

821. Had Intel disclosed to Plaintiffs and Minnesota Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that, in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Minnesota Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

822. Intel acted intentionally, knowingly, and maliciously to violate Minnesota's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs' and Minnesota Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

823. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

824. Plaintiffs and Minnesota Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief and attorneys' fees and costs.

MISSISSIPPI SUBCLASS COUNT XXVII

MISSISSIPPI CONSUMER PROTECTION ACT

Miss. Code § 75-24-1 *et seq.*

825. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

826. The non-entity Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Mississippi, and/or on behalf of the Mississippi Subclass.

827. Intel is a "person," as defined by Miss. Code § 75-24-3.

828. Intel advertised, offered, or sold goods or services in Mississippi and engaged in trade or commerce directly or indirectly affecting the people of Mississippi, as defined by Miss. Code § 75-24-3.

829. Prior to filing suit, Plaintiffs made reasonable attempts to resolve their claims via informal dispute resolution processes; however, such processes were unsuccessful.

830. The above-described conduct violated Miss. Code Ann. § 75-24-5(2), including: representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have; representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and advertising goods or services with intent not to sell them as advertised.

831. Intel intended to mislead Plaintiffs and Mississippi Subclass members and induce them to rely on its misrepresentations and omissions.

832. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

833. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects; that the CPU Defects allowed unauthorized access to confidential information; that necessary mitigations to address the Defects would result in significant CPU performance degradation; and that, in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

834. Had Intel disclosed to Plaintiffs and Mississippi Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that, in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Mississippi Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

835. Intel acted intentionally, knowingly, and maliciously to violate Mississippi's Consumer Protection Act, and recklessly disregarded Plaintiffs' and Mississippi Subclass members'

rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

836. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Mississippi Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

837. Intel's violations present a continuing risk to Plaintiffs and Mississippi Subclass members as well as to the general public because, among other things, its omissions and misrepresentations have not been corrected.

838. Plaintiffs and Mississippi Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution and other relief under Miss. Code § 75-24-11, injunctive relief, punitive damages, and reasonable attorneys' fees and costs.

MISSOURI SUBCLASS COUNT XXVIII

MISSOURI MERCHANDISE PRACTICES ACT

Mo. Rev. Stat. § 407.010 *et seq.*

839. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

840. Plaintiffs bring this count on behalf of themselves and all members of theClass that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Missouri, and/or on behalf of the Missouri Subclass.

841. Intel is a "person" as defined by Mo. Rev. Stat. § 407.010(5).

842. Intel advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. § 407.010(4), (6) and (7).

843. Plaintiffs and Missouri Subclass members purchased or leased goods or services primarily for personal, family, or household purposes.

844. Intel engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), as described herein.

845. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects; that the CPU Defects allowed unauthorized access to confidential information; that necessary mitigations to address the Defects would result in significant CPU performance degradation; and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

846. Intel representations and omissions were material because they were likely to deceive reasonable consumers.

847. Intel intended to mislead Plaintiffs and Missouri Subclass members and induce them to rely on its misrepresentations and omissions.

848. Intel acted intentionally, knowingly, and maliciously to violate Missouri's Merchandise Practices Act, and recklessly disregarded Plaintiffs' and Missouri Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

849. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Missouri Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

850. Plaintiffs and Missouri Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

MONTANA SUBCLASS COUNT XXIX

MONTANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT

M.C.A. § 30-14-101 *et seq.*

851. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

852. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Montana, and/or on behalf of the Montana Subclass.

853. Intel is a "person" as defined by MCA § 30-14-102(6).

854. Plaintiffs and Montana Subclass members are "consumers" as defined by M.C.A. § 30-14-102(1).

855. Intel advertised, offered, or sold goods or services in Montana and engaged in trade or commerce directly or indirectly affecting the people of Montana, as defined by M.C.A. § 30-14-102(8).

856. Intel engaged in unfair and deceptive acts and practices in the conduct of trade or commerce, in violation M.C.A. § 30-14-103, as described herein.

857. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

858. Had Intel disclosed to Plaintiffs and Montana Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that, in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Montana Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

859. Intel's acts described above are unfair and Plaintiffs and Montana Subclass members have lost money as a result of these practices. Intel's acts are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers. Indeed, Intel lulled consumers into thinking its CPUs were secure and fast, but the flaws in the CPUs allowed for significant security issues, which Intel knew, should have known about, or was reckless in not knowing about when it sold the CPUs. Intel knew, should have known, or was reckless in not knowing that it was exposing Plaintiffs

and absent Montana Subclass members to significant security problems with their most sensitive data and yet failed to inform consumers about those significant security issues. Thereafter, Intel put the onus on consumers to fix the defects by requiring the installation of patches which affected the core functionality of the CPUs.

860. Intel acted intentionally, knowingly, and maliciously to violate Montana's Unfair Trade Practices and Consumer Protection Act, and recklessly disregarded Plaintiffs' and Montana Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

861. As a direct and proximate result of Intel's unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, Plaintiffs and absent Montana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

862. Plaintiffs and Montana Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of $500 each, treble damages, restitution, attorneys' fees and costs, injunctive relief, and other relief that the Court deems appropriate.

NEBRASKA SUBCLASS COUNT XXX

NEBRASKA CONSUMER PROTECTION ACT

Neb. Rev. Stat. § 59-1601 *et seq.*

863. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

864. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Nebraska, and/or on behalf of the Nebraska Subclass.

865. Intel and absent Nebraska Subclass members are each a "person" as defined by Neb. Rev. Stat. § 59-1601(1).

866. Intel advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska, as defined by Neb. Rev. Stat. § 59-1601.

867. Intel engaged in unfair and deceptive acts and practices in conducting trade and commerce, in violation of Neb. Rev. Stat. § 59-1602, as described herein.

868. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

869. As a direct and proximate result of Intel's unfair and deceptive acts and practices, Plaintiffs and absent Nebraska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

870. Intel's unfair and deceptive acts and practices complained of herein affected the public interest, including the large percentage of Nebraskans who have purchased and/or used Intel CPUs.

871. Plaintiffs and Nebraska Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, the greater of either (1) actual damages or (2) $1,000 each, civil penalties, and reasonable attorneys' fees and costs.

NEBRASKA SUBCLASS COUNT XXXI

NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT

Neb. Rev. Stat. § 87-301 *et seq.*

872. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

873. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Nebraska, and/or on behalf of the Nebraska Subclass.

874. Intel and Nebraska Subclass members are each a "person" as defined by Neb. Rev. Stat. § 87-301(19).

875. Intel advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska.

876. Intel engaged in deceptive trade practices in the course of its business, in violation of Neb. Rev. Stat. §§ 87-302(a)(5), (8), and (10), including by: representing that goods and services have characteristics, uses, benefits, or qualities that they do not have; representing that goods and services are of a particular standard, quality, or grade if they are of another; and advertising its goods and services with intent not to sell them as advertised and in a manner calculated or tending to mislead or deceive.

877. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

878. Intel intended to mislead Plaintiffs and Nebraska Subclass members and induce them to rely on its misrepresentations and omissions.

879. Had Intel disclosed to Plaintiffs and Nebraska Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that, in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Nebraska Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

880. Intel acted intentionally, knowingly, and maliciously to violate Nebraska's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs' and Nebraska Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

881. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and Nebraska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

882. Intel's deceptive trade practices complained of herein affected consumers at large, including the large percentage of Nebraskans who purchased and/or used Intel CPUs.

883. Plaintiffs and Nebraska Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, civil penalties, and attorneys' fees and costs.

NEVADA SUBCLASS COUNT XXXII

NEVADA DECEPTIVE TRADE PRACTICES ACT

Nev. Rev. Stat. Ann. § 598.0903 *et seq.*

884. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

885. Plaintiffs bring this count on behalf of themselves and all members of theClass that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Nevada, and/or on behalf of the Nevada Subclass.

886. Intel advertised, offered, or sold goods or services in Nevada and engaged in trade or commerce directly or indirectly affecting the people of Nevada.

887. Intel engaged in deceptive trade practices in the course of its business or occupation, in violation of Nev. Rev. Stat. §§ 598.0915 and 598.0923, including: knowingly making a false representation as to the characteristics, uses, and benefits of goods or services for sale in violation of Nev. Rev. Stat. § 598.0915(5); representing that goods or services for sale are of a particular standard, quality, or grade when Intel knew or should have known that they are of another standard, quality, or grade, in violation of Nev. Rev. Stat. § 598.0915(7); advertising goods or services with intent not to sell them as advertised, in violation of Nev. Rev. Stat § 598.0915(9); failing to disclose a material fact in connection with the sale of goods or services ,in violation of Nev. Rev. Stat. § 598.0923(A)(2); and violating state and federal statutes or regulations relating to the sale of goods or services, in violation of Nev. Rev. Stat. § 598.0923(A)(3).

888. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

889. Had Intel disclosed to Plaintiffs and Nevada Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Nevada Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

890. Intel acted intentionally, knowingly, and maliciously to violate Nevada's Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs' and Nevada Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

891. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Nevada Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

892. Plaintiffs and Nevada Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, and attorneys' fees, and costs.

NEW HAMPSHIRE SUBCLASS COUNT XXXIII

NEW HAMPSHIRE CONSUMER PROTECTION ACT

N.H.R.S.A. § 358-A *et seq.*

893. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

894. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in New Hampshire, and/or on behalf of the New Hampshire Subclass.

895. Intel is a "person" under N.H.R.S.A. §§ 358-A:1(I) and 358-A:2.

896. Intel advertised, offered, or sold goods or services in New Hampshire and engaged in trade or commerce directly or indirectly affecting the people of New Hampshire, as defined by N.H.R.S.A. § 358-A:1(II).

897. Intel engaged in unfair and deceptive acts or practices in the ordinary conduct of its trade or business, in violation of N.H.R.S.A. § 358-A:2, including: representing that its goods or services have characteristics, uses, or benefits that they do not have, in violation of N.H.R.S.A. § 358-A:2(V); representing that its goods or services are of a particular standard or quality if they are of another, in violation of N.H.R.S.A. § 358-A:2(VII); and advertising its goods or services with intent not to sell them as advertised, in violation of N.H.R.S.A. § 358-A:2(IX).

898. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

899. Intel acted intentionally, knowingly, and maliciously to violate New Hampshire's Consumer Protection Act, and recklessly disregarded Plaintiffs' and New Hampshire Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice

that the CPUs were not as it advertised. Intel's acts and practices went beyond the realm of strictly private transactions.

900. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent New Hampshire Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

901. Plaintiffs and New Hampshire Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, equitable relief (including injunctive relief), restitution, civil penalties, and attorneys' fees and costs.

NEW JERSEY SUBCLASS COUNT XXXIV

NEW JERSEY CONSUMER FRAUD ACT,

N.J. Stat. Ann. § 56:8-1 *et seq.*

902. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

903. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in New Jersey, and/or on behalf of the New Jersey Subclass.

904. Intel is a "person," as defined by N.J. Stat. Ann. § 56:8-1(d).

905. Intel sells "merchandise," as defined by N.J. Stat. Ann. § 56:8-1(c) & (e).

906. The New Jersey Consumer Fraud Act, N.J. Stat. § 56:8-1 *et seq.*, prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material

fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

907. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

908. Intel intended to mislead Plaintiffs and New Jersey Subclass members and induce them to rely on its misrepresentations and omissions.

909. Intel acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiffs' and New Jersey Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

910. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent New Jersey Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

911. Plaintiffs and New Jersey Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

NEW MEXICO SUBCLASS COUNT XXXV

NEW MEXICO UNFAIR PRACTICES ACT

N.M. Stat. Ann. § 57-12-2 *et seq.*

912. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

913. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in New Mexico, and/or on behalf of the New Mexico Subclass.

914. Intel is a "person" within the meaning of N.M. Stat. Ann. § 57-12-2.

915. Intel was engaged in "trade" and "commerce" within the meaning of N.M. Stat. Ann. § 57-12-2(C) when engaging in the conduct alleged.

916. The New Mexico Unfair Practices Act, N.M. Stat. Ann. § 57-12-2 *et seq.*, prohibits both unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce.

917. Intel engaged in unconscionable, unfair, and deceptive acts and practices in connection with the sale of goods or services in the regular course of its trade or commerce, including the following: knowingly representing that its goods and services have characteristics, benefits, or qualities that they do not have, in violation of N.M. Stat. Ann. § 57-12-2(D)(5); knowingly representing that its goods and services are of a particular standard or quality when they are of another, in violation of N.M. Stat. Ann. § 57-12-2(D)(7); knowingly using exaggeration, innuendo, or ambiguity as to a material fact or failing to state a material fact where doing so deceives or tends to deceive, in violation of N.M. Stat. Ann. § 57-12-2(D)(14); taking advantage of the lack of knowledge, experience, or capacity of its consumers to a grossly unfair degree to Plaintiffs' and the New Mexico Subclass's detriment, in violation of N.M. Stat. Ann. § 57-2-12(E)(1); and performing these acts and practices in a way that results in a gross disparity between the value received by Plaintiffs and the New Mexico Subclass and the price paid, to their detriment, in violation of N.M. Stat. § 57-2-12(E)(2).

918. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

919. Intel intended to mislead Plaintiffs and New Mexico Subclass members and induce them to rely on its misrepresentations and omissions.

920. Intel acted intentionally, knowingly, and maliciously to violate New Mexico's Unfair Practices Act, and recklessly disregarded Plaintiffs' and New Mexico Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

921. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent New Mexico Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

922. Plaintiffs and New Mexico Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages or statutory damages of $100 (whichever is greater), treble damages or statutory damages of $300 each (whichever is greater), and reasonable attorneys' fees and costs.

NEW YORK SUBCLASS COUNT XXXVI

NEW YORK GENERAL BUSINESS LAW

N.Y. Gen. Bus. Law § 349 *et seq.*

923. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

924. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in New York, and/or on behalf of the New York Subclass.

925. Intel engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, as described herein.

926. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

927. Intel acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiffs' and New York Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

928. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

929. Intel's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the millions of New Yorkers who purchased and/or used Intel CPUs.

930. The above deceptive and unlawful practices and acts by Intel caused substantial injury to Plaintiffs and absent New York Subclass members that they could not reasonably avoid.

931. Plaintiffs and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 each (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

NORTH CAROLINA SUBCLASS COUNT XXXVII

NORTH CAROLINA UNFAIR TRADE PRACTICES ACT

N.C. Gen. Stat. Ann. § 75-1.1 *et seq.*

932. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

933. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in North Carolina, and/or on behalf of the North Carolina Subclass.

934. Intel advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

935. Intel engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, as described herein.

936. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

937. Intel intended to mislead Plaintiffs and North Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

938. Had Intel disclosed to Plaintiffs and North Carolina Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result

in significant CPU performance degradation; and (iv) that, in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent North Carolina members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

939. Intel acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiffs' and North Carolina Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

940. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and North Carolina Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

941. Intel's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

942. Plaintiffs and North Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

NORTH DAKOTA SUBCLASS COUNT XXXVIII

NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT

N.D. Cent. Code § 51-15-01 *et seq.*

943. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

944. Plaintiffs bring this count on behalf of themselves and all members of thel Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in North Dakota, and/or on behalf of the North Dakota Subclass.

945. Intel, Plaintiffs, and each member of the North Dakota Subclass is a "person," as defined by N.D. Cent. Code § 51-15-01(4).

946. Intel sells and advertises "merchandise," as defined by N.D. Cent. Code § 51-15-01(3) and (5).

947. Intel advertised, offered, or sold goods or services in North Dakota and engaged in trade or commerce directly or indirectly affecting the people of North Dakota.

948. Intel engaged in deceptive, false, fraudulent, misrepresentative, unconscionable, and substantially injurious acts and practices in connection with the sale and advertisement of merchandise, in violation of N.D. Cent. Code § 51-15-01, as described herein.

949. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

950. Intel's above-described acts and practices caused substantial injury to Plaintiffs and North Dakota Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

951. Intel intended to mislead Plaintiffs and North Dakota Subclass members and induce them to rely on its misrepresentations and omissions.

952. Intel acted intentionally, knowingly, and maliciously to violate North Dakota's Unlawful Sales or Advertising Law, and recklessly disregarded Plaintiffs' and North Dakota Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

953. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent North Dakota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

954. Plaintiffs and North Dakota Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, restitution, treble damages, civil penalties, and attorneys' fees, costs, and disbursements.

OHIO SUBCLASS COUNT XXXIX

OHIO CONSUMER SALES PRACTICES ACT

Ohio Rev. Code § 1345.01 *et seq.*

955. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

956. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Ohio, and/or on behalf of the Ohio Subclass.

957. Plaintiffs and absent Ohio Subclass members are "persons," as defined by Ohio Rev. Code § 1345.01(B).

958. Intel was a "supplier" engaged in "consumer transactions," as defined by Ohio Rev. Code §§ 1345.01(A) & (C).

959. Intel advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

960. Intel engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code §§ 1345.02, including: representing that its goods, services, and intangibles had performance characteristics, uses, and benefits that it did not have, in violation of Ohio Rev. Code § 1345.02(B)(1); and representing that its goods, services, and intangibles were of a particular standard or quality when they were not, in violation of Ohio Rev. Code § 1345(B)(2).

961. Intel engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code Ann. § 1345.03, including: knowingly taking advantage of the inability of Plaintiffs and the absent members of the Ohio Subclass to reasonably protect their interest because of their ignorance of the issues discussed herein (Ohio Rev. Code Ann. § 1345.03(B)(1)); and requiring Plaintiffs and the absent members of the Ohio Subclass to enter into a consumer transaction on terms that Intel knew were substantially one-sided in its favor (Ohio Rev. Code Ann. § 1345.03(B)(5)).

962. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

963. Intel intended to mislead Plaintiffs and Ohio Subclass members and induce them to rely on its misrepresentations and omissions.

964. Intel acted intentionally, knowingly, and maliciously to violate Ohio's Consumer Sales Practices Act, and recklessly disregarded Plaintiffs' and Ohio Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

965. Intel's unfair, deceptive, and unconscionable acts and practices complained of herein affected the public interest, including the millions of Ohioans who purchased and/or used Intel CPUs.

966. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

967. Plaintiffs and the Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including declaratory and injunctive relief, the greater of actual and treble damages or statutory damages, attorneys' fees and costs, and any other appropriate relief.

OHIO SUBCLASS COUNT XL

OHIO DECEPTIVE TRADE PRACTICES ACT

Ohio Rev. Code § 4165.01 *et seq.*

968. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

969. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Ohio, and/or on behalf of the Ohio Subclass.

970. Intel, Plaintiffs, and absent Ohio Subclass members are each a "person," as defined by Ohio Rev. Code § 4165.01(D).

971. Intel advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

972. Intel engaged in deceptive trade practices in the course of its business and vocation, in violation of Ohio Rev. Code § 4165.02, including: representing that its goods and services have characteristics, uses, benefits, or qualities that they do not have, in violation of Ohio Rev. Code § 4165.02(A)(7); representing that its goods and services are of a particular standard or quality when they are of another, in violation of Ohio Rev. Code § 4165.02(A)(9); and advertising its goods and services with intent not to sell them as advertise, in violation of Ohio Rev. Code § 4165.02(A)(11).

973. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

974. Intel intended to mislead Plaintiffs and Ohio Subclass members and induce them to rely on its misrepresentations and omissions.

975. Intel acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs' and Ohio Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

976. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

977. Plaintiffs and Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, attorneys' fees, and any other relief that is just and proper.

OKLAHOMA SUBCLASS COUNT XLI

OKLAHOMA CONSUMER PROTECTION ACT

Okla. Stat. Tit. 15, § 751 *et seq.*

978. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

979. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Oklahoma, and/or on behalf of the Oklahoma Subclass.

980. Intel is a "person," as meant by Okla. Stat. tit. 15, § 752(1).

981. Intel's advertisements, offers of sales, sales, and distribution of goods, services, and other things of value constituted "consumer transactions" within the meaning of Okla. Stat. tit. 15, § 752(2).

982. Intel, in the course of its business, engaged in unlawful practices in violation of Okla. Stat. tit. 15, § 753, including the following: making false representations, knowingly or with reason to know, as to the characteristics, uses, and benefits of the subjects of its consumer transactions, in violation of Okla. Stat. tit. 15, § 753(5); representing, knowingly or with reason to know, that the subjects of its consumer transactions were of a particular standard when they were of another, in violation of Okla. Stat. tit 15, § 753(7); advertising, knowingly or with reason to know, the subjects of its consumer transactions with intent not to sell as advertised, in violation of Okla. Stat. tit 15, § 753 (8); committing unfair trade practices that offend established public policy and were immoral,

unethical, oppressive, unscrupulous, and substantially injurious to consumers, as defined by section 752(14), in violation of Okla. Stat. tit. 15, § 753(20); and committing deceptive trade practices that deceived or could reasonably be expected to deceive or mislead a person to the detriment of that person as defined by section 752(13), in violation of Okla. Stat. tit. 15, § 753(20).

983. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

984. Intel intended to mislead Plaintiffs and Oklahoma Subclass members and induce them to rely on its misrepresentations and omissions.

985. Intel acted unfairly in failing to disclose the Defects to Plaintiffs and Oklahoma Subclass members because it was in a superior position to provide that information to the Plaintiffs and Oklahoma Subclass members and ordinary, reasonable consumers would not be able to know that the CPUs contained defects or required patches to operate in a secure manner absent Intel's disclosure.

986. Had Intel disclosed to Plaintiffs and Oklahoma Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Oklahoma Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

987. The above unlawful practices and acts by Intel were immoral, unethical, oppressive, unscrupulous, unfair, and substantially injurious. These acts caused substantial injury to Plaintiffs and absent Oklahoma Subclass members.

988. Intel acted intentionally, knowingly, and maliciously to violate Oklahoma's Consumer Protection Act, and recklessly disregarded Plaintiffs' and Oklahoma Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

989. As a direct and proximate result of Intel's unfair and deceptive acts and practices, Plaintiffs and Oklahoma Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

990. Like other Oklahoma Subclass members, Plaintiffs experienced actual losses in connection with the CPU defects and patching due to those defects. Those losses include, but are not limited to, loss of time in patching computers as a result of the security flaws, loss or compromise of data due to security flaws, and/or mitigation costs—damages which can be proven at trial.

991. Plaintiffs and Oklahoma Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, civil penalties, and attorneys' fees and costs.

OREGON SUBCLASS COUNT XLII

OREGON UNLAWFUL TRADE PRACTICES ACT

Or. Rev. Stat. § 646.608 *et seq.*

992. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

993. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Oregon, and/or on behalf of the Oregon Subclass.

994. Intel is a "person," as defined by Or. Rev. Stat. § 646.605(4).

995. Intel engaged in the sale of "goods and services," as defined by Or. Rev. Stat. § 646.605(6)(a).

996. Intel sold "goods or services," as defined by Or. Rev. Stat. § 646.605(6)(a). The CPUs at issue may be sold individually or inside of a machine. Intel CPUs are often a motivating factor for an individual's purchase of particular machine, and, at any rate, Intel routinely sells large quantities of CPUs individually.

997. Intel advertised, offered, or sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the people of Oregon.

998. Intel engaged in unlawful practices in the course of its business and occupation, in violation of Or. Rev. Stat. § 646.608, included the following: representing that its goods and services have approval, characteristics, uses, benefits, and qualities that they do not have, in violation of Or. Rev. Stat. § 646.608(1)(e); representing that its goods and services are of a particular standard or quality if they are of another, in violation of Or. Rev. Stat. § 646.608(1)(g); advertising its goods or services with intent not to provide them as advertised, in violation of Or. Rev. Stat. § 646.608(1)(i); and concurrent with tender or delivery of its goods and services, failing to disclose any known material Defect, in violation of Or. Rev. Stat. § 646.608(1)(t).

999. Intel's representations and omissions were material because they were likely to deceive reasonable consumers. Specifically, Intel's conduct included:

1000. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with the Defects, which go toward their central functionality, resulting in security risks, compromising confidential information, and—if patched—significantly degrading CPU performance thereby, again, impacting their central functionality, so that consumers did not receive the benefit of their bargain;

1001. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

1002. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

1003. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

1004. Making affirmative public representations about the speed of Intel CPUs while knowing that, in order for those CPUs to offer security for consumers' data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

1005. Concealing and/or failing to disclose material facts, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

1006. Intel intended to mislead Plaintiffs and Oregon Subclass members and induce them to rely on its misrepresentations and omissions.

1007. Had Intel disclosed to Plaintiffs and Oregon Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and Oregon Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

1008. Intel acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act, and recklessly disregarded Plaintiffs' and Oregon Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

1009. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Oregon Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs with installed Intel CPUs, and increased time and expense in dealing with performance and security issues.

1010. Plaintiffs and Oregon Subclass members seek all monetary and non-monetary relief allowed by law, including equitable relief, actual damages or statutory damages of $200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

PENNSYLVANIA SUBCLASS COUNT XLIII

PENNSYLVANIA UNFAIR TRADE PRACTICES AND

CONSUMER PROTECTION LAW

73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq.*

1011. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

1012. The non-entity Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Pennsylvania, and/or on behalf of the Pennsylvania Subclass.

1013. Intel is a "person," as meant by 73 Pa. Cons. Stat. § 201-2(2).

1014. Plaintiffs and absent Pennsylvania Subclass members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

1015. Intel engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following: representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v)); representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201-2(4)(vii)); and advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

1016. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

1017. Intel intended to mislead Plaintiffs and Pennsylvania Subclass members and induce them to rely on its misrepresentations and omissions.

1018. Had Intel disclosed to Plaintiffs and Pennsylvania Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Pennsylvania Alabama Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

1019. Intel acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiffs and absent Pennsylvania Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

1020. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and Pennsylvania Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing their personal CPUs, and increased time and expense in dealing with performance and security issues.

1021. Plaintiffs and Pennsylvania Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater),

treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

RHODE ISLAND SUBCLASS COUNT XLIV

RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT

R.I. Gen. Laws § 6-13.1 *et seq.*

1022. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

1023. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Rhode Island, and/or on behalf of the Rhode Island Subclass.

1024. Plaintiffs and Rhode Island Subclass members are each a "person," as defined by R.I. Gen. Laws § 6-13.1-1(3).

1025. Plaintiffs and Rhode Island Subclass members purchased goods and services for personal, family, or household purposes.

1026. Intel advertised, offered, or sold goods or services in Rhode Island and engaged in trade or commerce directly or indirectly affecting the people of Rhode Island, as defined by R.I. Gen. Laws § 6-13.1-1(5).

1027. Intel engaged in unfair and deceptive acts and practices, in violation of R.I. Gen. Laws § 6-13.1-2, including: representing that its goods and services have characteristics, uses, and benefits that they do not have (R.I. Gen. Laws § 6-13.1-52(6)(v)); representing that its goods and services are of a particular standard or quality when they are of another (R.I. Gen. Laws § 6-13.1-52(6)(vii)); advertising goods or services with intent not to sell them as advertised (R.I. Gen. Laws § 6-13.1-52(6)(ix)); engaging in any other conduct that similarly creates a likelihood of confusion

or misunderstanding (R.I. Gen. Laws § 6-13.1-52(6)(xii)); engaging in any act or practice that is unfair or deceptive to the consumer (R.I. Gen. Laws § 6-13.1-52(6)(xiii)); and using other methods, acts, and practices that mislead or deceive members of the public in a material respect (R.I. Gen. Laws § 6-13.1-52(6)(xiv)).

1028. Intel's representations and omissions were material because they were likely to deceive reasonable consumers. Specifically, Intel's actions included:

1029. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with the Defects, which go toward their central functionality, resulting in security risks, compromising confidential information, and—if patched—significantly degrading CPU performance thereby, again, impacting their central functionality, so that consumers did not receive the benefit of their bargain;

1030. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

1031. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

1032. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

1033. Making affirmative public representations about the speed of Intel CPUs while knowing that, in order for those CPUs to offer security for consumers' data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

1034. Concealing and/or failing to disclose material facts, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU

performance degradation, and that in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

1035. Intel intended to mislead Plaintiffs and Rhode Island Subclass members and induce them to rely on its misrepresentations and omissions.

1036. Intel acted intentionally, knowingly, and maliciously to violate Rhode Island's Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs' and absent Rhode Island Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

1037. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Rhode Island Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

1038. Plaintiffs and Rhode Island Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $200 per Subclass Member (whichever is greater), punitive damages, injunctive relief, other equitable relief, and attorneys' fees and costs.

SOUTH CAROLINA SUBCLASS COUNT XLV

SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT

S.C. Code Ann. § 39-5-10 *et seq.*

1039. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

1040. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in South Carolina, and/or on behalf of the South Carolina Subclass.

1041. Intel is a "person," as defined by S.C. Code Ann. § 39-5-10(a).

1042. South Carolina's Unfair Trade Practices Act (SC UTPA) prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." S.C. Code Ann. § 39-5-20.

1043. Intel advertised, offered, or sold goods or services in South Carolina and engaged in trade or commerce directly or indirectly affecting the people of South Carolina, as defined by S.C. Code Ann. § 39-5-10(b).

1044. Intel's acts and practices had, and continue to have, the tendency or capacity to deceive.

1045. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

1046. Intel intended to mislead Plaintiffs and South Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

1047. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects; that the CPU Defects allowed unauthorized access to confidential information; that necessary mitigations to address the Defects would result in significant CPU performance degradation; and that, in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making

partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

1048. Had Intel disclosed to Plaintiffs and South Carolina Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent South Carolina Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

1049. Intel's business acts and practices offend an established public policy, or are immoral, unethical, or oppressive.

1050. Intel's unfair and deceptive acts or practices adversely affected the public interest because such acts or practices have the potential for repetition; Intel engages in such acts or practices as a general rule; and such acts or practices impact the public at large, including millions of South Carolina Subclass members that purchased and/or used an Intel CPU.

1051. Intel unfair and deceptive acts or practices have the potential for repetition because the same kinds of actions occurred in the past, as described herein, thus making it likely that these acts or practices will continue to occur if left undeterred. Additionally, Intel's policies and procedures create the potential for recurrence of the complained-of business acts and practices.

1052. Intel violations present a continuing risk to Plaintiffs and absent South Carolina Subclass members as well as to the general public.

1053. Intel intended to mislead Plaintiffs and South Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

1054. Intel acted intentionally, knowingly, and maliciously to violate South Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiffs' and absent South Carolina Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised. In light of this conduct, punitive damages would serve the interest of society in punishing and warning others not to engage in such conduct and would deter Intel and others from committing similar conduct in the future.

1055. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent South Carolina Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

1056. Plaintiffs and South Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including damages for their economic losses, treble damages, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

SOUTH DAKOTA SUBCLASS COUNT XLVI

SOUTH DAKOTA DECEPTIVE TRADE PRACTICES AND CONSUMER PROTECTION ACT

S.D. Codified Laws § 37-24-1 *et seq.*

1057. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

1058. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in South Dakota, and/or on behalf of the South Dakota Subclass.

1059. Intel is a "person," as defined by S.D. Codified Laws § 37-24-1(8).

1060. Intel advertises and sells "merchandise," as defined by S.D. Codified Laws § 37-24-1(6), (7), & (13).

1061. Intel advertised, offered, or sold goods or services in South Dakota and engaged in trade or commerce directly or indirectly affecting the people of South Dakota, as defined by S.D. Codified Laws § 37-24-1(6), (7), & (13).

1062. Intel knowingly engaged in deceptive acts or practices, misrepresentation, concealment, suppression, or omission of material facts in connection with the sale and advertisement of goods or services, in violation of S.D. Codified Laws § 37-24-6, as described herein.

1063. Intel intended to mislead Plaintiffs and South Dakota Subclass members and induce them to rely on its misrepresentations and omissions.

1064. Intel representations and omissions were material because they were likely to deceive reasonable consumers.

1065. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects; that the CPU Defects allowed unauthorized access to confidential information; that necessary mitigations to address the Defects would result in significant CPU performance degradation; and that, in designing its CPUs, Intel had failed to take

measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

1066. Had Intel disclosed to Plaintiffs and South Dakota Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent South Dakota Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

1067. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent South Dakota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

1068. Intel's violations present a continuing risk to Plaintiffs and absent South Dakota Subclass members as well as to the general public.

1069. Plaintiffs and South Dakota Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, and reasonable attorneys' fees and costs.

TENNESSEE SUBCLASS COUNT XLVII

TENNESSEE CONSUMER PROTECTION ACT

Tenn. Code Ann. § 47-18-101 *et seq.*

1070. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

1071. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Tennessee, and/or on behalf of the Tennessee Subclass.

1072. Intel is a "person," as defined by Tenn. Code § 47-18-103(13).

1073. Plaintiffs and absent Tennessee Subclass members are "consumers," within the meaning of Tenn. Code § 47-18-103(2).

1074. Intel advertised and sold "goods" or "services" in "consumer transaction[s]," as defined by Tenn. Code §§ 47-18-103(7), (18) & (19).

1075. Intel advertised, offered, or sold goods or services in Tennessee and engaged in trade or commerce directly or indirectly affecting the people of Tennessee, as defined by Tenn. Code §§ 47-18-103(7), (18) & (19). Furthermore, Intel's acts or practices affected the conduct of trade or commerce, within the meaning and scope of Tenn. Code § 47-18-104.

1076. Intel intended to mislead Plaintiffs and Tennessee Subclass members and induce them to rely on its misrepresentations and omissions.

1077. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

1078. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects; that the CPU Defects allowed unauthorized access to confidential information; that necessary mitigations to address the Defects would result in significant CPU performance degradation; and that, in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

1079. Had Intel disclosed to Plaintiffs and Tennessee Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Tennessee Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

1080. Intel's "unfair" acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1081. The injury to consumers was and is substantial because it was non-trivial and non-speculative and involved a monetary injury. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1082. Consumers could not have reasonably avoided injury because Intel's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers as described herein, Intel created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1083. Intel's business practices had no countervailing benefit to consumers or to competition.

1084. By misrepresenting and omitting material facts, Intel violated the following provisions of Tenn. Code § 47-18-104(b): representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have; representing that goods or services are of a particular standard, quality or grade, if they are of another; advertising goods or services with intent not to sell them as advertised; and representing that a consumer transaction confers or involves rights, remedies or obligations that it does not have or involve. Intel's actions included:

1085. Knowingly designing, developing, manufacturing, advertising, and selling CPUs with the Defects, which go toward their central functionality, resulting in security risks,

compromising confidential information, and—if patched—significantly degrading CPU performance thereby, again, impacting their central functionality, so that consumers did not receive the benefit of their bargain;

1086. Permitting instruction execution in the Intel CPUs without first performing and enforcing the appropriate memory access checks as a means to increase processor speed and, accordingly, putting profits over the safety of consumer data;

1087. Failing to take steps to secure the CPU architecture from cache side-channel attacks;

1088. Making affirmative public representations about the security of Intel CPUs while, at the same time, not ensuring that safety is a priority in its devices;

1089. Making affirmative public representations about the speed of Intel CPUs while knowing that, in order for those CPUs to offer security for consumers' data, they would need to be patched, which would reduce processor speed or leave systems corrupted and still vulnerable; and

1090. Concealing and/or failing to disclose material facts, including but not limited to, that the CPUs contained the Defects, that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks.

1091. Intel acted intentionally, knowingly, and maliciously to violate Tennessee's Consumer Protection Act, and recklessly disregarded Plaintiffs' and absent Tennessee Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

1092. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Tennessee Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

1093. Intel's violations present a continuing risk to Plaintiffs and absent Tennessee Subclass members as well as to the general public.

1094. Plaintiffs and Tennessee Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, treble damages for each willful or knowing violation, attorneys' fees and costs, and any other relief that is necessary and proper.

TEXAS SUBCLASS COUNT XLVIII

TEXAS DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT

Texas Bus. & Com. Code § 17.41 *et seq.*

1095. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

1096. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Texas, and/or on behalf of the Texas Subclass.

1097. Intel is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

1098. Plaintiffs and absent Texas Subclass members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

1099. Intel advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

1100. Intel engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including: representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have; representing that goods or services are of a particular standard, quality or grade, if they are of another; and advertising goods or services with intent not to sell them as advertised.

1101. Intel intended to mislead Plaintiffs and Texas Subclass members and induce them to rely on its misrepresentations and omissions.

1102. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

1103. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects; that the CPU Defects allowed unauthorized access to confidential information; that necessary mitigations to address the Defects would result in significant CPU performance degradation; and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

1104. Had Intel disclosed to Plaintiffs and Texas Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Texas Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

1105. Intel engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Intel engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

1106. Plaintiffs and absent Texas Subclass members lacked knowledge about the above business practices, omissions, and misrepresentations because this information was known exclusively by Intel.

1107. Intel intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Intel's conduct is glaringly noticeable, flagrant, complete, and unmitigated.

1108. Intel acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiffs' and absent Texas

Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

1109. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Texas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

1110. Intel's violations present a continuing risk to Plaintiffs and Texas Subclass members as well as to the general public.

1111. Intel received notice pursuant to Tex. Bus. & Com. Code Ann. § 17.505 concerning its wrongful conduct as alleged herein by Plaintiffs and absent Texas Subclass members. Sending pre-suit notice pursuant to Tex. Bus. & Com. Code Ann. § 17.505, however, is an exercise in futility for Plaintiffs because Intel has already been informed of the allegedly unfair and unlawful conduct as described herein as of the date of the first-filed action among the cases centralized in this multidistrict litigation, and has yet to offer Texas Subclass members remedy in accordance with similar consumer protection statute.

1112. Plaintiffs and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages, damages for mental anguish, treble damages for each act committed intentionally or knowingly, court costs, reasonably and necessary attorneys' fees, injunctive relief, and any other relief which the Court deems proper.

UTAH SUBCLASS COUNT XLIX

UTAH CONSUMER SALES PRACTICES ACT

Utah Code § 13-11-1 *et seq.*

1113. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

1114. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Utah, and/or on behalf of the Utah Subclass.

1115. Intel is a "person," as defined by Utah Code § 13-11-1(5).

1116. Intel is a "supplier," as defined by Utah Code § 13-11-1(6), because it regularly solicits, engages in, or enforces "consumer transactions," as defined by Utah Code § 13-11-1(2).

1117. Intel engaged in deceptive and unconscionable acts and practices in connection with consumer transactions, in violation of Utah Code §§ 13-11-4 and 13-11-5, as described herein.

1118. Intel intended to mislead Plaintiffs and Utah Subclass members and induce them to rely on its misrepresentations and omissions.

1119. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

1120. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects; that the CPU Defects allowed unauthorized access to confidential information; that necessary mitigations to address the Defects would result in significant CPU performance degradation; and that, in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because

both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

1121. Had Intel disclosed to Plaintiffs and Texas Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that, in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Utah Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

1122. Intel intentionally or knowingly engaged in deceptive acts or practices, violating Utah Code § 13-11-4(2) by: indicating that the subject of a consumer transaction has sponsorship, approval, performance characteristics, accessories, uses, or benefits, if it has not; indicating that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not; indicating that the subject of a consumer transaction has been supplied in accordance with a previous representation, if it has not; indicating that the subject of a consumer transaction will be supplied in greater quantity (e.g., more data security) than the supplier intends.

1123. Intel engaged in unconscionable acts and practices that were oppressive and led to unfair surprise, as shown in the setting, purpose, and effect of those acts and practices.

1124. In addition, there was an overall imbalance in the obligations and rights imposed by the consumer transactions in question, based on the mores and industry standards of the time and place where they occurred. There is a substantial imbalance between the obligations and rights of consumers, such as Plaintiffs and absent Utah Subclass members, who purchase CPUs based upon the publicly-available information in the marketplace, and Intel, which has exclusive or superior knowledge of any Defects in those devices and software developed to address those Defects.

1125. Intel's acts and practices were also procedurally unconscionable because consumers, including Plaintiffs and absent Utah Subclass members, had no practicable option but to purchase CPUs based upon publicly available information, despite Intel's omissions and misrepresentations.

1126. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Utah Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

1127. Intel's violations present a continuing risk to Plaintiffs and absent Utah Subclass members as well as to the general public.

1128. Under Utah Code § 13-11-19, Plaintiffs and Utah Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, statutory damages of $2,000 per violation, amounts necessary to avoid unjust enrichment, injunctive relief, and reasonable attorneys' fees and costs.

VERMONT SUBCLASS COUNT L

VERMONT CONSUMER FRAUD ACT

Vt. Stat. Ann. tit. 9, § 2451 *et seq.*

1129. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

1130. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Vermont, and/or on behalf of the Vermont Subclass.

1131. Plaintiffs and Vermont Subclass members are "consumers," as defined by Vt. Stat. Ann. tit. 9, § 2451a(a).

1132. Intel's conduct as alleged herein related to "goods" or "services" for personal, family, or household purposes, as defined by Vt. Stat. Ann. tit. 9, § 2451a(b).

1133. Intel is a "seller," as defined by Vt. Stat. Ann. tit. 9, § 2451a(c).

1134. Intel advertised, offered, or sold goods or services in Vermont and engaged in trade or commerce directly or indirectly affecting the people of Vermont.

1135. Intel engaged in unfair and deceptive acts or practices, in violation of Vt. Stat. tit. 9, § 2453(a), as described herein.

1136. Intel intended to mislead Plaintiffs and Vermont Subclass members and induce them to rely on its misrepresentations and omissions.

1137. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

1138. Under the circumstances, consumers had a reasonable interpretation of Intel's representations and omissions.

1139. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects; that the CPU Defects allowed unauthorized access to confidential information, that necessary mitigations to address the Defects would result in significant CPU performance degradation; and that, in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

1140. Intel's acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1141. The injury to consumers was and is substantial because it was non-trivial and non-speculative; and involved a concrete monetary injury. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1142. Consumers could not have reasonably avoided injury because Intel's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers, Intel created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1143. Intel's business practices had no countervailing benefit to consumers or to competition.

1144. Intel is presumed, as a matter of law under Vt. Stat. Ann. tit. 9, § 2457, to have intentionally violated the Vermont Consumer Protection Act because it failed to sell goods or services in the manner and of the nature advertised or offered.

1145. Intel acted intentionally, knowingly, and maliciously to violate Vermont's Consumer Fraud Act, and recklessly disregarded Plaintiffs' and Vermont Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

1146. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and Vermont Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

1147. Plaintiffs and Vermont Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, restitution, actual damages, disgorgement of profits, treble damages, punitive/exemplary damages, and reasonable attorneys' fees and costs.

VIRGINIA SUBCLASS COUNT LI

VIRGINIA CONSUMER PROTECTION ACT

Va. Code Ann. § 59.1-196 *et seq.*

1148. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

1149. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Virginia, and/or on behalf of the Virginia Subclass.

1150. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

1151. Intel is a "person" as defined by Va. Code Ann. § 59.1-198.

1152. Intel is a "supplier," as defined by Va. Code Ann. § 59.1-198.

1153. Intel engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198. Intel advertised, offered, or sold goods or services used primarily for personal, family or household purposes.

1154. Intel engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, described herein.

1155. Intel intended to mislead Plaintiffs and Virginia Subclass members and induce them to rely on its misrepresentations and omissions.

1156. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

1157. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects; that the CPU Defects allowed unauthorized access to confidential information; that necessary mitigations to address the Defects would result in significant CPU performance degradation, and that in designing its CPUs, Intel had failed to take

measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

1158. Had Intel disclosed to Plaintiffs and Virginia Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Virginia Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

1159. The above-described deceptive acts and practices also violated the following provisions of Va. Code § 59.1-200(A): misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits; misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised.

1160. Intel acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Plaintiffs' and absent Virginia Subclass members' rights.

Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised. An award of punitive damages would serve to punish Intel for its wrongdoing and warn or deter others from engaging in similar conduct.

1161. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Virginia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

1162. Intel's violations present a continuing risk to Plaintiffs and absent Virginia Subclass members as well as to the general public.

1163. Plaintiffs and Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of $1,000 per violation if the conduct is found to be willful or, in the alternative, $500 per violation; restitution; injunctive relief; punitive damages; and attorneys' fees and costs.

WASHINGTON SUBCLASS COUNT LII

WASHINGTON CONSUMER PROTECTION ACT

Wash. Rev. Code Ann. § 19.86.020 *et seq.*

1164. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

1165. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Washington, and/or on behalf of the Washington Subclass.

1166. Intel is a "person," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

1167. Intel advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

1168. Intel engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, as described herein.

1169. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects; that the CPU Defects allowed unauthorized access to confidential information; that necessary mitigations to address the Defects would result in significant CPU performance degradation; and that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

1170. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

1171. Intel acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiffs' and absent Washington Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

1172. Intel's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest

impact, and/or injured persons and had and has the capacity to injure persons. Furthermore, its conduct affected the public interest, including the at least hundreds of thousands of Washingtonians affected by Intel's deceptive business practices.

1173. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and Washington Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues

1174. Plaintiffs and Washington Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

WEST VIRGINIA SUBCLASS COUNT LIII

WEST VIRGINIA CONSUMER CREDIT AND PROTECTION ACT

W. Va. Code § 46A-6-101 *et seq.*

1175. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

1176. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in West Virginia, and/or on behalf of the West Virginia Subclass.

1177. Plaintiffs and West Virginia Subclass members are "consumers," as defined by W. Va. Code § 46A-6-102(2).

1178. Intel engaged in "consumer transactions," as defined by W. Va. Code § 46A-6-102(2).

1179. Intel advertised, offered, or sold goods or services in West Virginia and engaged in trade or commerce directly or indirectly affecting the people of West Virginia, as defined by W. Va. Code § 46A-6-102(6).

1180. Intel received notice pursuant to W. Va. Code § 46A-6-106(c) concerning its wrongful conduct as alleged herein by Plaintiffs and West Virginia Subclass members. Sending pre-suit notice pursuant to W. Va. Code § 46A-6-106(c), however, is an exercise in futility for Plaintiffs, because, despite being on knowledge of the deceptive acts and practices complained of herein in this lawsuit as of the date of the first-filed action among the cases centralized in this multidistrict litigation, Intel has not cured its unfair and deceptive acts and practices.

1181. Intel engaged in unfair and deceptive business acts and practices in the conduct of trade or commerce, in violation of W. Va. Code § 46A-6-104, as described herein.

1182. Intel's unfair and deceptive acts and practices also violated W. Va. Code § 46A-6-102(7), including: representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have; representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model if they are of another; advertising goods or services with intent not to sell them as advertised; engaging in any other conduct that similarly creates a likelihood of confusion or of misunderstanding; using deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of goods or services, whether or not any person has in fact been misled, deceived or damaged thereby; and advertising, displaying, publishing, distributing, or causing to be advertised, displayed, published, or distributed in any manner, statements and representations with regard to the sale of goods that are false, misleading or

deceptive or that omit to state material information which is necessary to make the statements therein not false, misleading, or deceptive.

1183. Intel's unfair and deceptive acts and practices were unreasonable when weighed against the need to develop or preserve business, and were injurious to the public interest, under W. Va. Code § 46A-6-101.

1184. Intel's acts and practices were additionally "unfair" under W. Va. Code § 46A-6-104 because they caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1185. The injury to consumers from Intel's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1186. Consumers could not have reasonably avoided injury because Intel's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers, Intel created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1187. Intel's business practices had no countervailing benefit to consumers or to competition.

1188. Intel's acts and practices were additionally "deceptive" under W. Va. Code § 46A-6-104 because Intel made representations or omissions of material facts that misled or were likely to mislead reasonable consumers, including Plaintiffs and absent West Virginia Subclass members.

1189. Intel intended to mislead Plaintiffs and absent West Virginia Subclass members and induce them to rely on its misrepresentations and omissions.

1190. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

1191. Intel had a duty to disclose material facts to consumers, including but not limited to, that the CPUs contained the Defects; that the CPU Defects allowed unauthorized access to confidential information; that necessary mitigations to address the Defects would result in significant CPU performance degradation; and that, in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks. These material facts should have been disclosed because both security and performance are central to CPU functionality; because Intel had exclusive or superior knowledge regarding such facts; and because Intel suppressed these facts while making partial representations as alleged herein. Moreover, these material facts should have been disclosed because they were contrary to Intel's representations about the CPUs.

1192. Had Intel disclosed to Plaintiffs and West Virginia Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs

and absent West Virginia Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

1193. Intel's omissions were legally presumed to be equivalent to active misrepresentations because Intel intentionally prevented Plaintiffs and West Virginia Subclass members from discovering the truth regarding Intel's CPU Defects.

1194. Intel acted intentionally, knowingly, and maliciously to violate West Virginia's Consumer Credit and Protection Act, and recklessly disregarded Plaintiffs' and West Virginia Subclass members' rights. Intel's unfair and deceptive acts and practices were likely to cause serious harm, and Intel knew that its deceptive acts would cause harm based upon its business practices and exclusive knowledge of the omissions and misrepresentations herein.

1195. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent West Virginia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

1196. Intel's violations present a continuing risk to Plaintiffs and absent West Virginia Subclass members as well as to the general public.

1197. Plaintiffs and West Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $200 per violation under W. Va. Code § 46A-6-106(a), restitution, injunctive and other equitable relief, punitive damages, and reasonable attorneys' fees and costs.

WISCONSIN SUBCLASS COUNT LIV

WISCONSIN DECEPTIVE TRADE PRACTICES ACT

Wis. Stat. § 100.18 *et seq.*

1198. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

1199. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Wisconsin, and/or on behalf of the Wisconsin Subclass.

1200. Intel is a "person, firm, corporation or association," as defined by Wis. Stat. § 100.18(1).

1201. Plaintiffs and absent Wisconsin Subclass members are members of "the public," as defined by Wis. Stat. § 100.18(1).

1202. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by Intel to members of the public for sale, use, or distribution, Intel made, published, circulated, placed before the public or caused (directly or indirectly) to be made, published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations to the public that contained assertions, representations, or statements of fact that were untrue, deceptive, and/or misleading, in violation of Wis. Stat. § 100.18(1).

1203. Intel also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as advertised, in violation of Wis. Stat. § 100.18(9).

1204. Those advertisements were placed in Wisconsin by Intel or through retailers and other third parties who sold products containing Intel CPUs and were provided information for

advertisements relating to the CPUs. That Intel placed and made advertisements in Wisconsin is evident by the fact that Intel was able to sell, based upon information and belief, thousands of CPUs in the state. Indeed, discovery will demonstrate how may advertisements Intel made to or targeted at Wisconsin to the Wisconsin Subclass.

1205. Intel intended to mislead Plaintiffs and Wisconsin Subclass members and induce them to rely on its misrepresentations and omissions.

1206. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

1207. Intel's had a duty to disclose the above-described facts due to the circumstances of this case, including its exclusive knowledge of the CPU Defects, its concealment regarding same, and its incomplete representations regarding its CPUs.

1208. Intel's failure to disclose the above-described facts is the same as actively representing that those facts do not exist.

1209. Intel acted intentionally, knowingly, and maliciously to violate the Wisconsin Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs' and Wisconsin Subclass members' rights. Intel's knowledge of the CPUs' performance and security issues put it on notice that the CPUs were not as it advertised.

1210. As a direct and proximate result of Intel's deceptive acts or practices, Plaintiffs and absent Wisconsin Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with CPU performance and security issues.

1211. Intel had an ongoing duty to all Intel customers under Wis. Stat. § 100.18 to refrain from deceptive acts, practices, plans, and schemes.

1212. Plaintiffs and Wisconsin Subclass members seek all monetary and non-monetary relief allowed by law, including damages, reasonable attorneys' fees, and costs under Wis. Stat. § 100.18(11)(b)(2), injunctive relief, and punitive damages.

WYOMING SUBCLASS COUNT LV

WYOMING CONSUMER PROTECTION ACT

Wyo. Stat. Ann. § 40-12-101 *et seq.*

1213. Plaintiffs reallege and incorporate the preceding paragraphs as if fully set forth herein.

1214. Plaintiffs bring this count on behalf of themselves and all members of the Class that purchased or leased one or more Intel CPUs or one or more devices containing an Intel CPU in Wyoming, and/or on behalf of the Wyoming Subclass.

1215. Intel is a "person" as defined by Wyo. Stat. Ann. § 42-12-102(i).

1216. Plaintiffs and Wyoming Subclass members engaged in "consumer transactions" as defined by Wyo. Stat. Ann. § 40-12-102(ii).

1217. Intel is engaged in an "uncured unlawful deceptive trade practice" in accordance with Wyo. Stat. Ann. § 40-12-105 in that it had actual notice of its deceptive acts and practices when the first action of the cases centralized in this multidistrict litigation was file. It has not, however, offered to adjust or modified the consumer transactions at issue in this case, nor has it offered to rescind the consumer transactions. Consequently, pre-suit notice to Intel pursuant to Wyo. Stat. Ann. § 40-12-109 was an exercise in futility.

1218. Intel advertised, offered, or sold goods or services in Wyoming, and engaged in trade or commerce directly or indirectly affecting the people of Wyoming.

1219. Intel engaged in deceptive acts and practices in the conduct of trade or commerce, in violation of the Wyoming Consumer Protection Act, Wyo. Stat. Ann. §§ 40-12-101, *et seq.*, including: representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have; representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce.

1220. Intel's representations and omissions were material because they were likely to deceive reasonable consumers.

1221. Intel intended to mislead Plaintiffs and Wyoming Subclass members and induce them to rely on its misrepresentations and omissions.

1222. Had Intel disclosed to Plaintiffs and Wyoming Subclass members material facts, including but not limited to, that: (i) its CPUs contained the Defects; (ii) the CPU Defects allowed unauthorized access to confidential information; (iii) mitigations to address the Defects would result in significant CPU performance degradation; and (iv) that in designing its CPUs, Intel had failed to take measures to protect confidential information from attacks by unauthorized users while knowing that its CPUs were vulnerable to such attacks, Intel would have been unable to sell as many CPUs that it did or at the price such CPUs were sold. Instead, Intel represented that its CPUs were continually improving in speed and performed better than other processors on the market. Plaintiffs and absent Wyoming Subclass members acted reasonably in relying on Intel's misrepresentations and omissions, the truth of which they could not have discovered.

1223. Intel acted intentionally, knowingly, and maliciously to violate the Wyoming Consumer Protection Act, and recklessly disregarded Plaintiffs' and Wyoming Subclass members' rights. Intel's knowledge of the CPUs' security and performance issues put it on notice that the CPUs were not as it advertised.

1224. As a direct and proximate result of Intel's deceptive acts and practices, Plaintiffs and absent Wyoming Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in purchasing the CPUs, and increased time and expense in dealing with performance and security issues.

1225. Intel's deceptive acts and practices caused substantial injury to Plaintiffs and absent Wyoming Subclass members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

1226. Plaintiffs and the Wyoming Subclass seek all monetary and non-monetary relief allowed by law, actual damages, injunctive relief, attorneys' fees, costs, and any other relief that is just and proper.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all other Class members, respectfully request that the Court enter an Order:

A. Declaring that this action is a proper class action, certifying the Class and/or Subclasses as requested herein, designating Plaintiffs as Class Representatives, and appointing Plaintiffs' attorneys as Class Counsel;

B. Enjoining Intel from continuing the unfair business practices alleged in this Complaint;

C. Ordering Intel to pay actual and statutory damages (including punitive damages) and restitution to Plaintiffs and the other Class members, as allowable by law;

D. Ordering Intel to pay both pre- and post-judgment interest on any amounts awarded;

E. Ordering Intel to pay attorneys' fees and costs of suit; and

F. Ordering such other and further relief as may be just and proper.

JURY DEMAND

Plaintiffs hereby demand a trial by jury on all issues so triable.

DATED this 29th day of May, 2020.

STOLL STOLL BERNE LOKTING
& SHLACHTER P.C.

By: s/ Jennifer S. Wagner
Steve D. Larson, OSB No. 863540
Jennifer S. Wagner, OSB No. 024470

209 SW Oak Street, Suite 500
Portland, Oregon 97204
Telephone: (503) 227-1600
Email: slarson@stollberne.com
jwagner@stollberne.com

Interim Plaintiffs' Liaison Counsel

Christopher A. Seeger (*pro hac vice*)
SEEGER WEISS LLP
55 Challenger Road
Ridgefield Park, NJ 07660
Telephone: (212) 584-0700
Email: cseeger@seegerweiss.com

Rosemary M. Rivas (*pro hac vice*)
LEVI & KORSINSKY LLP
388 Market Street, Suite 1300
San Francisco, CA 94111
Telephone: (415) 291-2420
Email: rrivas@zlk.com

Interim Co-Lead Plaintiffs' Counsel

Gayle M. Blatt (*pro hac vice*)
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Email: gmb@cglaw.com

Stuart A. Davidson (*pro hac vice*)
ROBBINS GELLER RUDMAN & DOWD LLP
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Telephone: (561) 750-3000
Email: sdavidson@rgrdlaw.com

Melissa R. Emert (*pro hac vice*)
STULL, STULL, & BRODY
6 East 45th Street
New York City, NY 10017
Telephone: (212) 687-7230
Email: memert@ssbny.com

Richard M. Hagstrom (*pro hac vice*)
HELLMUTH & JOHNSON PLLC
8050 West 78th Street
Edina, MN 55439
Telephone: (952) 941-4005
Email: rhagstrom@hjlawfirm.com

Jennifer L. Joost (*pro hac vice*)
KESSLER TOPAZ MELTZER & CHECK LLP
One Sansome Street, Suite 1850
San Francisco, CA 94104
Telephone: (415) 400-3000
Email: jjoost@ktmc.com

Adam J. Levitt (*pro hac vice*)
DICELLO LEVITT & CASEY LLC
Ten North Dearborn Street, Eleventh Floor
Chicago, IL 60602
Telephone: (312) 214-7900
Email: alevitt@dlcfirm.com

Charles E. Schaffer (*pro hac vice*)
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
Email: cschaffer@lfsblaw.com

Interim Plaintiffs' Steering Committee